Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS

Aplicación de las directivas de la NTP ISO/IEC 27001:2014 para la implementación de un sistema de gestión de seguridad de la información en el Centro de Gestión Tributaria de Chiclayo

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

PRESENTADO POR:

Nikitín Alarce Edquén Bonilla

Freddy Nilton Torres Chanamé

ASESOR:

Dr. Ing. Ernesto Karlo Celi Arévalo

Lambayeque – Perú

2019

Universidad Nacional Pedro Ruiz Gallo

Facultad De Ingeniería Civil De Sistemas Y De Arquitectura

Escuela Profesional De Ingeniería De Sistemas

TESIS

Aplicación de las directivas de la NTP ISO/IEC 27001:2014 para la implementación de un sistema de gestión de seguridad de la información en el Centro de Gestión Tributaria de Chiclayo

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

APROBADO POR LOS MIEMBROS DE JURADO DE TESIS

Mg. Ing. Roberto Carlos Arteaga Lora
Presidente

Mg. Ing. Frank Richard Rodríguez Chirinos
Secretario

Ing. Oscar Efraín Capuñay Uceda
Vocal

Dr. Ing. Ernesto Karlo Celi Arévalo
Asesor

Bach. Nikitín Alarce Edquén Bonilla
Responsable

Bach. Freddy Nilton Torres Cháñame
Responsable

Lambayeque – Perú
2019

DEDICATORIA

A mi esposa María de Jesús Rivas Bravo por sus palabras y tiempo necesario para realizarme profesionalmente.

A mi hija Nikoll Aracely Edquén Rivas, por ser mi fuente de inspiración y superación en la vida a seguir para adelante, también por sus ocurrencias suscitadas durante el desarrollo de la tesis.

A mis padres por haberme formado con valores y haber brindado su apoyo incondicional durante mi desarrollo profesional.

A toda mi familia que directa o indirectamente fueron instrumentos de apoyo para el desarrollo y culminación de esta tesis.

A mis amigos, compañeros y a todas aquellas personas que de una u otra manera han contribuido en el logro de mis objetivos.

Nikitín Alarce Edquén Bonilla

Mi tesis la dedico con todo mi amor y cariño a mi amada esposa Viviana Azabache por su sacrificio y comprensión durante todos estos años y por creer en mí, aunque hemos pasado momentos difíciles siempre ha estado a mi lado brindándome su comprensión, cariño y amor.

A mis hijos Axel Xavier, Freddy Oziel y Alina Madeleine por ser fuente de mi motivación e inspiración para poder seguir superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

A mis queridos padres y hermanos quienes con sus palabras de aliento no me dejaban decaer para que siguiera adelante y siempre sea perseverante y cumpla con mis ideales.

A mis suegros que desde el primer día que llegue a formar parte de la familia me comprendieron y que me alentaron a seguir en la lucha por mis ideales.

A mis compañeros y amigos y amigos presentes y pasados, quienes sin esperar nada a cambio compartieron su conocimiento, alegrías y tristezas y a todas aquellas personas que durante estos años estuvieron a mi lado apoyándome y lograron que este sueño se haga realidad.

Freddy Nilton Torres Chanamé

AGRADECIMIENTOS

Mi agradecimiento a Dios, el que en todo momento está conmigo ayudándome a aprender de mis errores y a no cometerlos otra vez.

A mi asesor Dr. Ing. Celi Arévalo Ernesto Karlo por compartir sus conocimientos y apoyar en el desarrollo de la presente investigación.

Al Jefe de la Oficina de Tecnología de la Información del Centro de Gestión Tributaria de Chiclayo Ing. Denis Obando Fernández por su aceptación y tiempo dedicado en el desarrollo de la tesis.

Finalmente quiero agradecer a todas aquellas personas que de una u otra manera me ayudaron durante la elaboración de esta tesis. A todos gracias.

Nikitín Alarce Edquén Bonilla

Dios, es tu amor y tu bondad no tiene fin, me permites sonreír ante todos mis logros que son resultado de tu ayuda y cuando caigo y me pones a prueba, aprendo de mis errores y me doy cuenta que los pones frente mío para que mejore como ser humano y crezca de diversas maneras.

Agradezco también a mi Asesor de Tesis el Mag. Ing. Ernesto Celi Arévalo por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento científico, así como también por haberme tenido la paciencia para guiarme durante todo el desarrollo de la tesis.

Mi agradecimiento también va dirigido al Jefe de la Oficina de Tecnologías de la Información del Centro de Gestión Tributaria de Chiclayo por haber aceptado que se realice la tesis en dicha entidad.

Freddy Nilton Torres Chanamé

RESUMEN

La exigencia de la implementación de la norma técnica peruana NTP ISO/IEC 27001:2014 en las entidades públicas, nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas instituciones. Sin embargo, el desconocimiento de estos temas por parte de la dirección de estas entidades, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de los proyectos de tecnologías de la información.

El ONGEI, declara el uso obligatorio de esta norma, mediante la Resolución Ministerial N° 004-2016-PCM, para las instituciones públicas integrantes del Sistema Nacional de Informática, donde los entes dependientes de las municipalidades forman parte de ello. Por tal motivo, se hace importante desarrollar diversos planes de seguridad de la información en el Centro de Gestión Tributaria de Chiclayo (CGT) permitiendo proteger la información y los activos de información que se manejen dentro del flujo de los procesos más importantes en la entidad

Teniendo en cuenta esto, la presente investigación propone diseñar un modelo de un Sistema de Gestión de la Seguridad de la Información en el CGT, tomando como referencia la NTP ISO/IEC 27001:2014 y que además se acople a la normativa a la cual está sujeta la institución y que pueda, en un futuro, servir como referencia para la implementación del mismo.

En consecuencia, se realizaron varias reuniones con diversas áreas que permitirán definir el alcance y las políticas del SGSI en la entidad enfocándose en los procesos institucionales críticos en el CGT, posteriormente se realizó una serie de entrevistas que permitirán identificar y valorar los activos críticos de la organización así como identificar y evaluar los riesgos a los cuales estos están sometidos.

También cabe mencionar que en base al cronograma de implementación incremental del SGSI, propuesta por la ONGEI, nos enfocaremos en las dos primeras fases (Fase de organización y de planificación), para desarrollar el modelo del SGSI.

Palabras clave: seguridad de la información, Sistema de Gestión de Seguridad de la Información, ISO 27001

ABSTRACT

The requirement for the implementation of the Peruvian technical standard NTP ISO / IEC 27001: 2014 in public entities arises from the need to adequately manage the security of information in each of these institutions. However, the ignorance of these issues by the top management of these entities, has caused that the necessary measures are not taken to ensure the success of information technology projects.

The ONGEI, declares the mandatory use of this norm, through the Ministerial Resolution N ° 004-2016-PCM, for public institutions that are part of the National Computing System, where the entities dependent on the municipalities are part of it. For this reason, it is important to develop various information security plans at the Tax Administration Center of Chiclayo (CGT), allowing the protection of information and information assets that are managed within the flow of the most important processes in the entity.

Taking this into account, this research proposes to design a model of an Information Security Management System in the CGT, taking as reference the NTP ISO / IEC 27001: 2014 and that also fits the regulations to which it is subject the institution and that may, in the future, serve as a reference for the implementation of it.

As a result, several meetings were held with different areas that allowed defining the scope and policies of the ISMS in the entity, focusing on the critical institutional processes in the municipality. Subsequently, a series of interviews was conducted to identify and assess the critical assets of the institution. organization as well as identify and evaluate the risks to which they are subject.

It should also be mentioned that based on the incremental implementation schedule of the ISMS, proposed by the ONGEI, we will focus on the first two phases (Organization and planning phase), to develop the ISMS model.

Keywords: information security, Information Security Management System, ISO 27001

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

DATOS INFORMATIVOS

Título del proyecto

Aplicación de las directivas de la NTP ISO/IEC 27001:2014 para la implementación de un sistema de gestión de seguridad de la información en el Centro de Gestión Tributaria de Chiclayo

Código del proyecto

IS-2018-058

Personal investigador

Autor

- Nikitín Alarce Edquén Bonilla
  email: nedquenb@gmail.com, Teléfono: 979992908
- Freddy Nilton Torres Chanamé
  email: ftorres.satch@gmail.com, Teléfono: 944454101

Asesor

Dr. Ing. Celi Arévalo Ernesto Karlo

Línea de la investigación

Gobierno y gestión de tecnologías de información

Localidad o Institución donde se realizará el proyecto

Centro de Gestión Tributaria de Chiclayo, Provincia de Chiclayo, Departamento de Lambayeque

Fecha de presentación

Septiembre 2019

INTRODUCCION

Cada vez un mayor número de amenazas afectan a los sistemas de información constituyendo un riesgo sobre uno de los activos más críticos y vulnerables de las instituciones como es la información. Asegurar la disponibilidad, la confidencialidad y la conservación de los datos, es un servicio que debe brindar la organización por lo que la gestión de la seguridad de la información debe realizarse mediante un proceso documentado y conocido. Este proyecto describe un modelo de un sistema de seguridad de la información (SGSI) en el sector público para el Centro de Gestión Tributaria de Chiclayo (CGT) tomando como referencia la norma NTP ISO/IEC 27001:2014 para minimizar los riesgos reales y potenciales existentes en la institución.

Para describir dicho modelo, la presente investigación se estructura en los siguientes capítulos:

En el **capítulo I**, se presenta la problemática de esta investigación así como también una lista de inconvenientes encontrados en el CGT con respecto a la seguridad de la información.

En el **capítulo II**, presenta una revisión bibliográfica de los temas principales sobre los que se fundamente la propuesta metodológica, además hace referencia a los antecedentes y trabajos relacionados.

El **capítulo III**, describe la metodología propuesta que servirá de guía para la implementación del Sistema de Gestión de Seguridad de la Información para el CGT. Dicho marco metodológico se compone por 3 fases: El establecimiento del SGSI, planeamiento del SGSI y verificación del SGSI, en este último se pretende verificar si el desarrollo del plan de implementación del Sistema de Gestión de Seguridad de la Información propuesto considera los puntos descritos en la norma NTP ISO/IEC 27001:2014.

El **capítulo IV**, desarrolla el modelo de SGSI propuesto, tratando de cumplir con los objetivos de la investigación

Finalmente se presenta las conclusiones de la tesis a las que se ha llegado respecto al modelo del SGSI planteado para finalmente detallar las recomendaciones que podrán ser de gran apoyo al momento de realizar la implementación del sistema en el CGT.

I. EL PROBLEMA DE LA INVESTIGACIÓN

1.1. Descripción de la problemática institucional

El Centro de Gestión Tributaria de Chiclayo (CGT) es un organismo público descentralizado de la Municipalidad Provincial de Chiclayo, que goza de autonomía administrativa, económica y financiera, por lo que como organismo público debe ajustarse a las disposiciones establecidas para el sector público.

Se encarga de administrar y recaudar eficaz y eficientemente los tributos municipales, además de fomentar la consciencia tributaria y mejorar la percepción del servicio que ofrece, optimizando los procedimientos de cobranza, atención al contribuyente y fiscalización.

En su Plan Estratégico Institucional del Centro de Gestión Tributaria de Chiclayo, se han establecido 9 objetivos estratégicos generales, los cuales se analizaron respecto al impacto que tiene las TICs sobre éstas.

Tabla N° 1. Lineamientos del Plan Estratégico Institucional del CGT

CODIGO	OBJETIVOS ESTRATEGICO GENERALES	DESCRIPCIÓN
O.E.G.1	Maximizar la efectividad de la recaudación tributaria y no tributaria del CGT.	Concretar la máxima recaudación de las obligaciones tributarias y no tributarias, en los diversos estados de la gestión de cobranza.
O.E.G.2	Generar mayores ingresos propios adicionales para el Centro de Gestión Tributaria de Chiclayo	Incrementar la rentabilidad de la organización, a través de la reducción de la cartera morosa, saneamiento y generar ingresos adicionales.
O.E.G.3	Mejorar la percepción de servicio de la entidad.	Fortalecer la atención de servicio al administrado, buscando cumplir con las expectativas y necesidades del contribuyente.
O.E.G.4	Fortalecer la comunicación integral y la imagen institucional	Mejorar la percepción de la entidad frente a la sociedad.
O.E.G.5	Optimizar los procesos de todas las actividades administrativas y operacionales de la entidad.	La optimización de los procesos como objetivo busca favorecer la mayor eficacia y eficiencia en el uso de los recursos institucionales con la finalidad de alcanzar niveles altos en la prestación de los servicios.
O.E.G.6	Implementar soluciones tecnológicas que soporten la demanda de servicios.	La utilización de soluciones tecnológicas, como objetivo estratégico genera, surge ante el crecimiento de la demanda de servicios por parte del administrado.
O.E.G.7	Diseñar, implantar y desarrollar un modelo de organización y gestión estratégica de la función de recursos humanos que responden a los fines que se persigue como institución.	Diseñar y ejecutar un plan estratégico de recursos humanos.
O.E.G.8	Implantar para la toma de decisiones, sistemas de comunicación e información interna, revisión y control, mediante la modernización tecnológica e informática.	Mejorar la gestión de recursos humanos, a través del desarrollo y aplicación de soluciones tecnológicas.
O.E.G.9	Fortalecer la cultura y el clima organizacional de CGT.	A través de a cultura y clima organizacional, se transmite la filosofía institucional, y facilitan el trabajo, estableciendo relaciones laborales sanas armónicas que permitan generar compromiso del personal con la institución.

Fuente: Plan Estratégico Institucional 2016-2018

El impacto de las Tecnologías de Información en relación a los Objetivos Estratégicos Generales del CGT se muestra a continuación:

✓ Objetivos Institucionales **altamente** sensibles a las Tecnologías de la Información.	
✓ Objetivos Institucionales **medianamente** sensibles a las Tecnologías de la Información.	
✓ Objetivos Institucionales **poco** sensibles a las Tecnologías de la Información.	

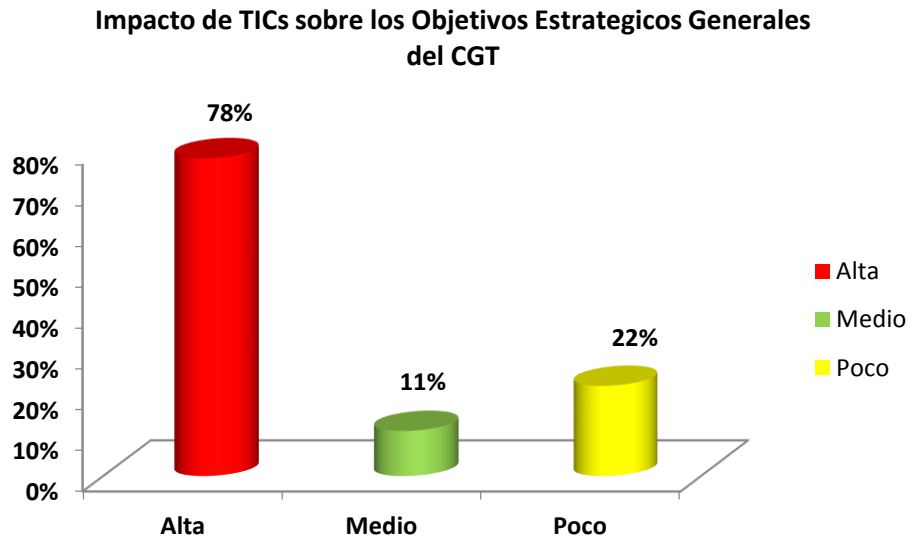


Figura N° 1. Impacto de TICs sobre los Objetivos Estratégicos Generales del CGT
Fuente: Elaboración Propia

Las tecnologías de la información tienen un 78% impacto para el logro de los objetivos estratégicos generales del CGT, es decir un nivel muy ALTO como apoyo en el desarrollo de los diferentes procesos de las unidades orgánicas de la institución; es decir de los 9 objetivos estratégicos generales, las TICs influyen de manera directo en 6 objetivos.

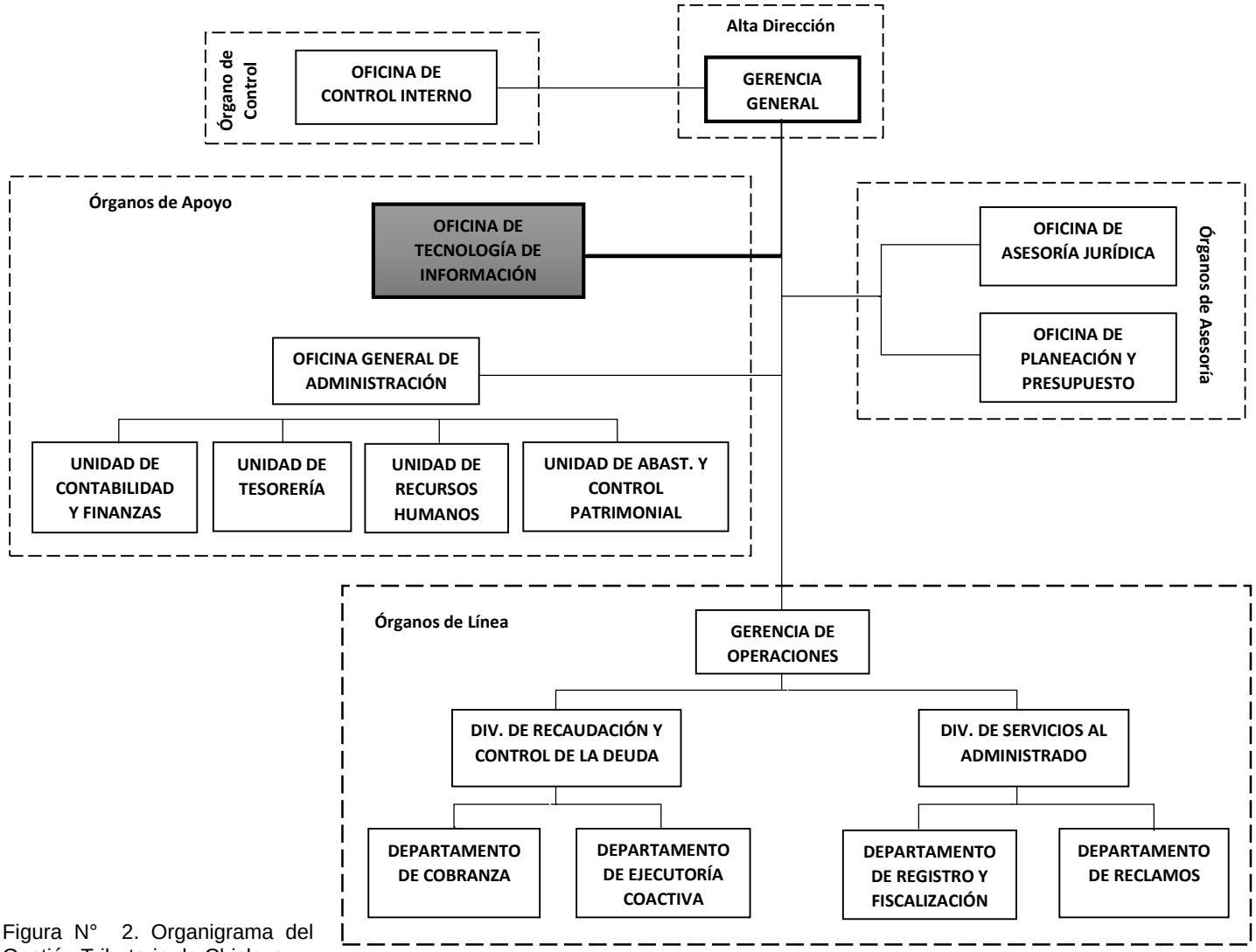


Figura N° 2. Organigrama del Centro de Gestión Tributaria de Chiclayo
Fuente: Manual de organización y funciones del Centro de Gestión Tributaria de Chiclayo (CGT Chiclayo, 2018)

1.2. Diagnóstico de la situación actual de la Oficina de Tecnologías de la información

El diagnóstico de la situación actual, nos permite realizar un análisis y las condiciones de las TICs del Centro de Gestión Tributaria de Chiclayo.

1.2.1. Evaluación de la Capacidad de Gestión TIC

Para la evaluación de la capacidad de gestión de TIC se ha aplicado un cuestionario de preguntas con respuestas cerradas que tuvieron una puntuación como sigue:

- Por cumplimiento de 1, Parcial de 0.5 y No cumplimiento de 0.
- La evaluación comprende el nivel de cumplimiento de 4 dominios: Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación. Esta evaluación comprende 30 procesos de control y 498 preguntas respecto a las actividades que se realizan en la Oficina de TI; estas preguntas han sido realizadas al Jefe de la Oficina de Tecnologías de Información y al Jefe del Área de Redes, Comunicaciones y Nuevas Tecnologías.

Nivel de Cumplimiento por Dominio

De manera global, luego del análisis del cumplimiento de los dominios propuestos en la Oficina de Tecnologías de Información del CGT, se puede observar que se cumple en un mayor porcentaje con respecto al dominio de SUBCONTRATACIÓN (74.89%), seguida por el dominio de Soporte (61.77%) y Plataforma Tecnológica (54.76%) y en un porcentaje menor pero por encima del promedio normal, es el dominio de Planeación y Organización (52.67%).

El nivel de cumplimiento de los 4 dominios propuestos en la Oficina de TI, se encuentran por encima del 50%, es decir en un nivel aceptable respecto al desarrollo de sus funciones.

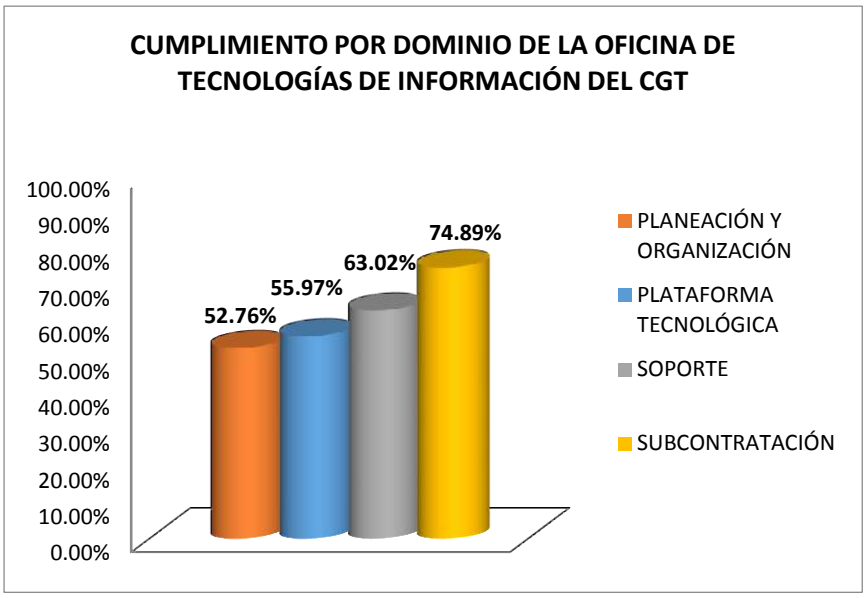


Figura N° 3. Cumplimiento por dominio de la oficina de tecnologías de información del CGT
Fuente: Elaboración Propia

PLANEACIÓN Y ORGANIZACIÓN

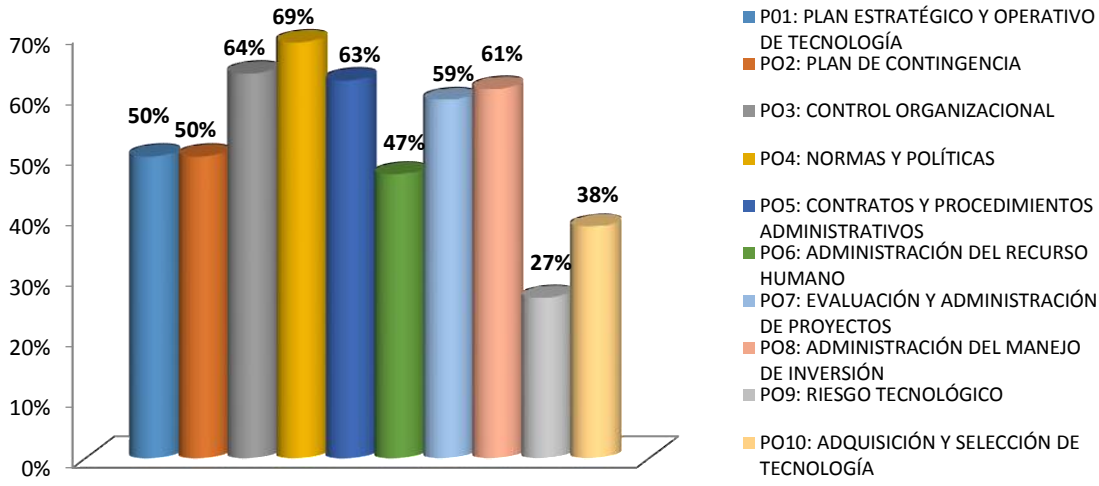


Figura N° 4. Nivel de cumplimiento del dominio Planeación y organización
Fuente: Elaboración Propia

PLATAFORMA TECNOLÓGICA

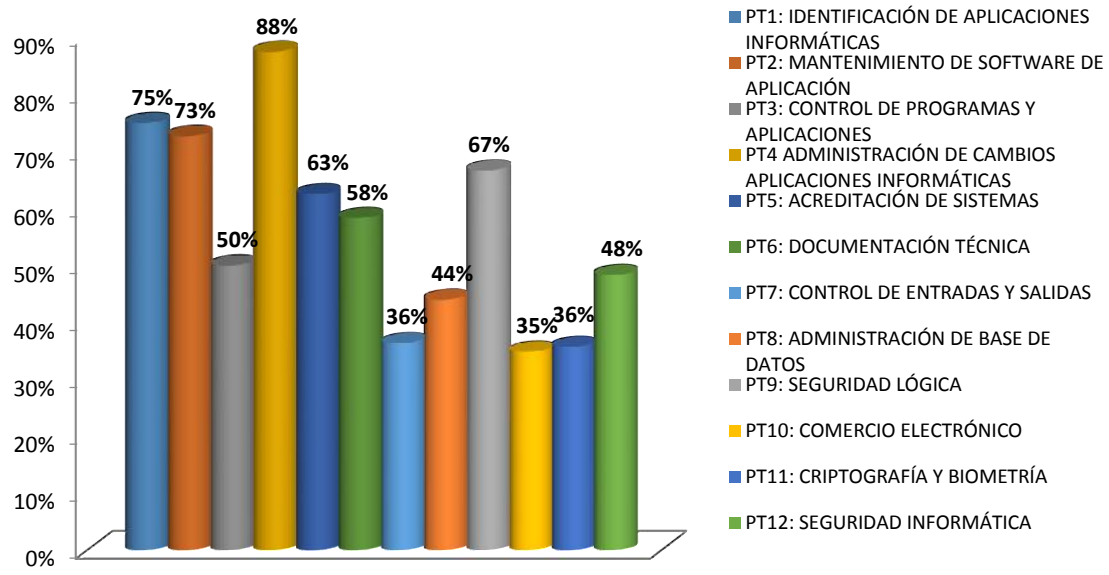


Figura N° 5. Nivel de cumplimiento del dominio Plataforma tecnológica
Fuente: Elaboración Propia

SOPORTE

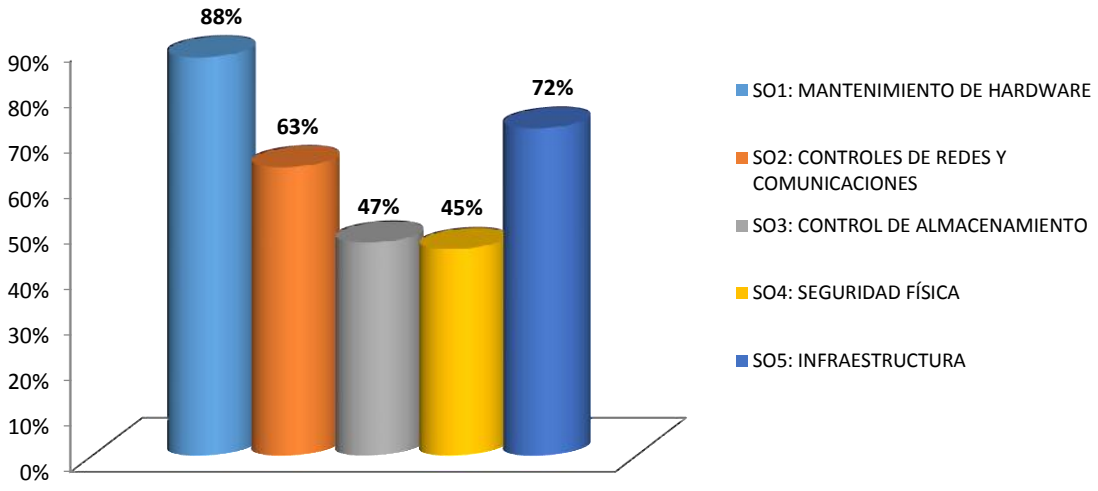


Figura N° 6. Nivel de cumplimiento del dominio Soporte
Fuente: Elaboración Propia

SUBCONTRATACIÓN

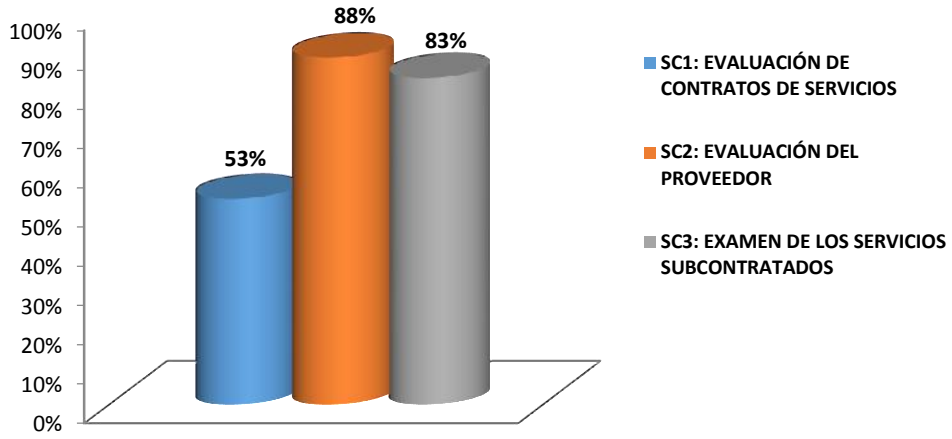


Figura N° 7. Nivel de cumplimiento del dominio Subcontratación
Fuente: Elaboración Propia

1.2.2. Diagnóstico de la Gestión de Oficina de Tecnologías de Información de acuerdo al cumplimiento de dominios

a. Planeación y Organización

En este dominio se ha evaluado las estrategias y tácticas adoptadas por la Oficina de TI, identificando de qué manera contribuye al logro de los objetivos planteados por la Alta Gerencia del Centro de Gestión Tributaria de Chiclayo.

El nivel de cumplimiento en Normas y Políticas (PO4) es de 69%, siendo aceptable, esto se debe a que el personal de la Oficina de TI vienen adecuando sus políticas y normas de CONFIDENCIALIDAD de acuerdo a las normas técnicas peruanas y leyes informáticas y plasmada en la Directiva de Seguridad de la Información, aprobado por la Alta Gerencia y aceptadas por la unidades orgánicas de la entidad, debiendo reforzar las siguientes tareas:

- Las políticas o normas emitidas deben ser actualizadas, por lo menos anualmente o al momento de presentarse cambios significativos en el ambiente operacional, para garantizar que sean funcionales y aplicables.
- Realizar reuniones en la exista la participación de las áreas especializadas de la institución en la creación y regulación de las normas y políticas, debiendo quedar plasmado en un documento los acuerdos tomados.

El procedimiento de Control Organizacional (PO3) tiene un cumplimento de 63%, debiendo coordinar con la Gerencia General del CGT en los siguientes puntos:

- Requerir personal con conocimientos en programación y soporte tecnológico, para evitar cargas excesivas en las actividades que se desempeñan en la Oficina de TI de la entidad.
- En la elaboración de un Plan de capacitaciones para el personal de la Oficina de TI y que éste responda a las necesidades de la entidad para el cumplimiento del Plan Estratégico de TI.

Seguido del procedimiento de Contratos y Procedimientos Administrativos (PO5) y con un nivel de cumplimiento de 63%; que en la gestión de un proyecto a desarrollar se toman en cuenta las directivas aprobadas (Directiva de Ciclo de Vida del Software), debiendo reforzar las siguientes tareas:

- Documentar los procedimientos de trabajos ejecutados por el personal de la Oficina de TI.
- Definir en los procedimientos escritos los horarios de trabajo para el personal de la Oficina de TI, considerando los cierres semanales, mensuales y anuales.
- Definir procedimientos de control manual o automático de la información que entra y sale de la Oficina de TI.
- Designar a un responsable oficial encargado de la Oficina para el Control la información para toda la organización, teniendo como una de sus funciones principales ser el enlace de la información entre TI y el resto de la organización.
- Mantener actualizada una póliza de seguro con cobertura para la pérdida de los equipos informáticos y medios de procesos de datos.
- Verificar las hojas de vida de los principales puestos de la Oficina de TI, para evaluar la capacidad y experiencia para desarrollar su puesto.

El proceso de Administración del Manejo de Inversión (PO8) tiene un cumplimiento de 61%, debiendo complementar las siguientes tareas:

- Definir procedimientos que permitan controlar, justificar y realizar el seguimiento correspondiente a los excesos en comparación al presupuesto asignado y cumplir con l proyección anual realizada.
-
- Realizar un analices de las licitaciones o matriz técnica de ofertas según proveedor y las condiciones del producto.
- Analizar los cambios en el presupuesto anual y anterior, debiendo estar en conformidad a las variaciones en los precios del mercado y necesidades de la entidad, debiendo justificar las variaciones considerables.
- Realizar un control adecuado de los costos en que incurre la Oficina de TI.
- Implementar procedimientos y políticas clara, definidas y documentadas respecto al monitoreo de costos.

El procedimiento que también tiene un nivel de cumplimiento aceptable es el de Evaluación y Administración de proyectos y Contratos (PO7) con un 59%, debiendo reforzar las siguientes tareas:

- Conformar un comité técnico evaluador de proyectos designando cargos y funciones de cada miembro; así mismo verificar si existe un libro de actas de los acuerdos y decisiones tomadas sobre los proyectos.
- Mantener la documentación histórica sobre la ejecución de los proyectos finalizados o en proceso.
- Tener en cuenta en las normativas internas de la entidad para la formulación de proyectos.
- Implementar mecanismos en coordinación con la Gerencia de la entidad, en la implementación de controles para evaluar periódicamente la ejecución del proyecto, de forma que permita evaluar la situación actual y efectuar las medidas correctivas necesarias, como cambios en el entorno del negocio y en la tecnología, para lograr la finalización del proyecto cumpliendo con las metas y objetivos requeridos.
- Considerar en la metodología de Administración de Proyectos los recursos logísticos.
- Considerar los estudios de factibilidad tecnológica de cada alternativa de forma que satisfaga los requerimientos de la entidad, para los proyectos de TI, que la entidad estime importantes.
- Considerar el estudio de costo beneficio de cada alternativa de forma que cubra los requerimientos de la entidad, para todos los proyectos de TI importantes que considera la entidad.
- En la planeación de los proyectos de TI , recalcar los siguientes puntos:
    - Implementar un Plan de Aseguramiento de calidad de sistemas.
    - Implementar un Plan de Pruebas (piloto, paralelo, modular, etc.)
    - Considerar un Plan de Capacitación.
    - Considerar un Plan de pruebas de estrés para las aplicaciones informáticas.
    - Mantener actualizada la documentación de las aplicaciones informáticas.
    - Considerar una programación financiera del proyecto, conforme a su avance.
- Conformar un Comité de Evaluación de proyectos con la responsabilidad de emitir actas que documenten los avances del proyecto y las decisiones tomadas en dicho comité.
- Tener bien definido la nueva tecnología a implantar y los riesgos asociados a cada una de ellas.

El proceso de Plan Estratégico y Operativo de Tecnología (PO1), tiene un 50% de cumplimiento; estando en el límite de aceptación, debiendo complementar los siguientes procedimientos:

- Incluir en el Plan Estratégico Institucional en la Plan estratégico de TI.
- Elaborar anualmente el Plan Operativo de TI.
- Implementar procedimientos que permitan realizar un seguimiento al cumplimiento de metas de los proyectos a corto plazo plasmados en Plan Operativo de TI.
- Implementar procedimientos que permitan realizar seguimiento a las actividades, periodos, grado de avance de las actividades del Plan Estratégico.
- Implementar procedimientos que permitan realizar el monitoreo sobre el desarrollo e implementación de los Planes de TI a corto y largo plazo para contribuir al cumplimiento de los objetivos y metas de dichos planes.
- Requerir en coordinación con la Gerencia General los recursos tecnológicos y humanos suficientes para el desarrollo de los proyectos.
- Mantener archivados los insumos o fuentes de información que se utilizan como base para la elaboración del Plan Estratégico de TI.

El procedimiento de Plan de Contingencia (PO2), tiene un cumplimiento de 50%, debiendo priorizar las siguientes tareas:

- Conformar un Comité de administración de desastres o de equipo de emergencia, debiendo estar incluidos en el Plan de Contingencia con sus funciones respectivas.
- Coordinar con la Gerencia General, en la adquisición de Servidor de contingencia para todas las aplicaciones críticas.
- Programar como mínimo 2 fechas al año para la puesta en práctica del plan de contingencia con la finalidad de fortalecer las áreas no funcionales.
- Implementar procedimientos para actualizar el manual, asimismo aplicar y distribuir las actualizaciones a los usuarios involucrados.
- Diseñar y adherir al plan de contingencia los planos del centro de cómputo, diagramas de cableado eléctrico, diagramas de red, diagramas de ductos e inventarios de hardware.
- Realizar copias de datos actualizados, programas y documentación técnica del sistema y almacenarlo en un lugar externo de la entidad.
- Capacitar al personal de la Oficina de TI y de la entidad respecto a los procedimientos establecidos para la continuidad de las operaciones en caso de desastres.
- Implementar un Centro de cómputo alterno o para la continuidad de operaciones, teniendo en cuenta las condiciones mínimas de seguridad física tales como: controles de acceso, piso elevado o protegido, controles de humedad, controles de temperatura, circuitos especializados, fuente interrumpida de energía, dispositivos de detección de agua, detectores de humo y un sistema adecuado de extinción de incendios.

El procedimiento de que está por debajo del promedio es el de Administración del recurso Humano (PO6) con un cumplimiento de 47%, debiendo tener en cuenta las siguientes tareas:

- Implementar procedimientos de evaluación al personal para garantizar un nivel aceptable de desempeño y cumplimiento de metas de la Oficina de TI.
- Implementar un plan de capacitaciones que esté orientado al giro de la entidad y la plataforma tecnológica con que cuenta la entidad.
- Realizar pruebas de entrenamiento cruzado, con la finalidad de disponer con personal de respaldo ante posible ausencia de personal clave.
- La jefatura de la Oficina de TI, debe implementar acciones oportunas y apropiadas con respecto a cambios de puestos y posibles renuncias del personal de TI.
- Coordinar con la Gerencia General del CGT para la contratación de personal, y cumplir con las funciones encomendadas.
- Implementar condiciones ambientales adecuadas, respecto a la seguridad de la Oficina de TI.

Otro proceso de menor cumplimiento tenemos el de Adquisición y Selección de Tecnología (PO10) con un cumplimiento de 38%, debiendo tener en cuenta las siguientes tareas:

- Conformar un Comité que evalué cada inversión que se realice en la adquisición de tecnología
- En cada adquisición de hardware o software revisar detalladamente los documentos fiscales para comprobar que los desembolsos realizados sean los facturados.
- Realizar un consenso con el personal responsable de la Oficina de TI, respecto a las condiciones contractuales brindadas por el proveedor al momento de la adquisición de tecnología.
- Tener elaborado un plan de migración de datos si lo realizará un tercero definiendo las responsabilidades a los integrantes para un mejor control.

Finalmente en este dominio el proceso de Riesgo Tecnológico (PO9) tiene un 27% siendo el de menor cumplimiento, debiendo priorizar las siguientes tareas:

- Conformar un Comité de Evaluación de Riesgo Tecnológico.
- El comité de Evaluación de Riesgos debe tener definido tareas que permitan identificar y medir los riesgos tecnológicos.
- Implementar controles y medidas de seguridad en las transferencias de datos que viajan a través de internet
- Realizar un análisis de los resultados emitidos por las auditorías externas que realizan a los sistemas con relación a objetivos, alcances, frecuencia, documentación apropiada, conclusiones y anexos y debatirlo con la Alta Gerencia

- Implementar mecanismos para medir la confidencialidad e integridad de los sistemas de información.
- Implementar mecanismos de seguridad en las transacciones enviadas o recibidas.
- Verificar dentro de los contratos de adquisición de software que no exista una cláusula que obligue a la entidad a disponer exclusivamente del producto por tiempo definido.
- Implementar políticas para monitoreo de funcionarios y empleados que se relacionen con las licitaciones y compras de equipos tecnológicos.
- Elaborar cuestionarios de evaluación de la percepción del público, respecto del servicio, estabilidad y calidad.

b. Plataforma Tecnológica

Ante el crecimiento de la entidad y dar un mejor servicio, la jefatura de la Oficina de TI, en éste dominio se evalúa los recursos tecnológicos que se emplea en la entidad, así mismo la seguridad informática, para lo cual se han determinado 12 procedimientos.

En este dominio el procedimiento el mayor cumplimiento es de Administración de cambios de aplicaciones informáticos (PT4) con 88%, debiendo:

- Complementar procedimientos para determinar el estatus de cada solicitud de cambios a realizados en los sistemas.
- Complementar procedimientos para evaluar las solicitudes identificadas como urgentes.

Otro procedimiento con mayor cumplimiento es Identificación de Aplicaciones Informáticas (PT1) con un 75%, debiendo tener en cuenta lo siguiente:

- Implementar un software de seguridad que controle las tablas sensibles y valide periódicamente contra los accesos no autorizados el cambio de configuración original.
- Complementar procedimientos de controles sobre los recursos compartidos en los equipos informáticos como: discos duros, carpetas o archivos.

El procedimiento de Mantenimiento de Software de Aplicación (PT2) tiene un 73% de cumplimiento:

- Consolidar responsabilidades y compromiso del comité responsable que aprueba cualquier proyecto de desarrollo, implementación o modificación.
- Debiendo complementar los mecanismos para identificar los requerimientos de seguridad y control interno para cada proyecto de desarrollo o modificación de sistemas de información, previo a su desarrollo.

- Considerar permanentemente aspectos básicos de seguridad y control interno del módulo a ser desarrollado o modificado.
- Implementar una metodología estándar para el desarrollo de un plan de pruebas, en donde se incluyan pruebas unitarias, pruebas de aplicación, pruebas de integración y pruebas de carga y estrés, para cada módulo.
- Complementar políticas y medidas de seguridad para prevenir divulgación de información sensible durante las pruebas.

El procedimiento de seguridad lógica (PT9) tiene un cumplimiento aceptable de un 67%, debiendo tener en cuenta los siguientes puntos:

- Implementar procedimientos para que el sistema operativo obligue al usuario a cambiar su contraseña de manera periódica.
- Implementar procedimientos que permita a los usuarios de los sistemas informar durante el proceso de identificación cuando fue su última conexión para ayudar a identificar posibles suplantaciones o accesos no autorizados.
- Implementar procedimientos que permitan a los equipos validar la identificación electrónica de las terminales que se agregan a la red.

El procedimiento de acreditación de sistemas (PT5) tiene un 63% de cumplimiento, debiendo tener en cuenta lo siguiente:

- Conformar un grupo de prueba independiente, diferente al de los desarrolladores, para las pruebas a los nuevos sistemas o a las modificaciones a los sistemas.
- Equipar un ambiente de prueba, el cual sea representativo del ambiente operacional futuro (por ejemplo: condiciones similares de seguridad, controles internos, cargas de trabajo, etc.)
- Implementar procedimientos para asegurar que la pruebas piloto o en paralelo sean llevadas a cabo con planes pre establecidos.
- Designar a un responsable para efectuar el trasladado de las nuevas aplicaciones o modificaciones de desarrollo a producción.

El procedimiento de Documentación Técnica (PT6), también tiene un 58% de cumplimiento, debiendo mejorar lo siguiente:

- Mantener en actualización constante el inventariado de las tablas de bases de datos con su respectiva descripción.
- Actualizar el diagrama entidad – relación por cada modificación que se realice.
- Documentar los manuales de usuario de los aplicativos puestos en producción por cada medicación que se realice.
- Implementar diccionarios de datos de las tablas o archivos que conforman los sistemas puestos en producción.

El procedimiento que se encuentra en promedio de cumplimiento, es el de Controles de programas y Aplicaciones (PT3) con un 50%, debiendo tener en cuenta los siguientes:

- Designar un personal de la Oficina de TI, con responsabilidades y funciones quien se encargue de revisar periódicamente los archivos log o bitácoras de los sistemas.
- Evaluación de un Plan para adquirir licencias de programas o software libre para el diagnóstico de la red de la entidad ante posibles fallas.

Tenemos los procedimientos que está por debajo del promedio en cumplimiento en éste dominio los cuales son importantes y se deben de mejorar, entre los cuales tenemos el de Seguridad de Informática (PT12) con 48% de cumplimiento debiendo mejorar las siguientes tareas:

- Adquirir software y hardware que permitan realizar pruebas de control a las amenazas externas, como hackers o espías.
- Desarrollar procedimientos para controlar las amenazas, por ejemplo: Sniffing, Frame Spoofing, Crack, hacking a un website, ingeniería social, caballos de troya, ataques de denegación de servicios, fake mail.
- Crear o incorporar funciones diferenciadas de los cargos siguientes: Administrador de Seguridad (Debe administrar altas, bajas y cambios de perfiles de usuarios, otorgar permisos de acceso a los recursos y pueda auditar a los usuarios), Administrador de red (Atender y monitorear la red, instalar y configurar los componentes de software y hardware, resolver problemas de ambiente y conexiones) , Administrador de Sistemas (Encargarse de la instalación de software de base, administración de recursos, sin acceso irrestricto a los datos).
- En la seguridad informática, implementar un Firewall, sistemas de actualizaciones automáticas de software, sistemas de control de la integridad de los servidores, paquetes.
- Redacción de informes de monitoreo y rastreo de las actividades de los usuarios administrativos y operativos a fin de detectar y corregir desviaciones en el uso correcto de la información, o en el cumplimiento de las normas y procedimientos asociados a la seguridad de la información.
- Complementar los controles lógicos y físicos para asegurar que sólo el personal autorizado pueda acceder a la información, dentro de los niveles de atención.
- Complementar políticas de evaluación en la destrucción de la información, especificando los medios a utilizar, los procedimientos a aplicar y la oportunidad en se ejecutará.

El procedimiento de Control de Entradas y salidas (PT7) tiene un 36% de cumplimiento, debiendo complementar las siguientes tareas:

- Implementar procedimientos de control que permita demostrar que la información ingresada a los sistemas se encuentra autorizada.
- Respecto a las salidas de datos, realizar inventarios de reportes, que identifique: nombre del programa, nombre del módulo, unidad destino, frecuencia de emisión y medio de emisión.
- Habilitar un área o lugar donde se resguarden los reportes confidenciales de manera que el personal no autorizado no pueda tener acceso a ellos.
- Designar funciones y responsabilidad a un personal de la Oficina de TI que se encargue de efectuar análisis general de los reportes con el objeto de determinar si hay reportes que puedan ser eliminados, fusionados, reagrupados, simplificados o si se requiere nuevos reportes.
- De los reportes de salida, deben ser etiquetados de manera individual o grupal de manera que se indique en el nombre del usuario, destino y el área o departamento al que pertenece.
- Consignar códigos que identifiquen el nivel de confidencialidad del reporte.
- Desarrollar procedimientos para la destrucción de reportes sobrantes o que no estén en uso.
- Implementar mecanismos de control para producir únicamente la cantidad requerida de reportes solicitados.

Otro procedimiento de menor cumplimento es el de Criptografía y Biometría (PT11) con un 36% siendo importante, debiendo tener en cuenta las siguientes tareas:

- Dentro de los tipos de cifrado de datos, se debe evaluar el que garantice mayor seguridad para envió de datos.
- Realizar el cifrado de datos bajo el ambiente PGP (pretty good privacy) de los servicios de correo electrónico, aplicaciones de mensajería instantánea o conexión a internet.
- Implementar procedimientos o herramientas para la autenticación mediante firma digital, que garantice la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación.
- Adquirir una Certificación Digital que contemple nombre de entidad, nombre de la Autoridad Certificadora, periodo de validez.
- Implementar políticas para el uso de biometría.
- Implementar procedimientos para crear o eliminar usuarios del sistema según el método biométrico desarrollado.

El procedimiento de Comercio Electrónico (PT10) tiene un 35% de cumplimiento respecto a las tareas, debiendo mejorar las siguientes:

- Dentro de los archivos de la Oficina de TI, se debe tener copia de los contratos de los proveedores de los servicios.
- Tener la documentación de las políticas configuración.

- Realizar reportes de caídas de los sistemas, para medir la frecuencia y la magnitud de las mismas.
- Designar a un personal de la Oficina de TI como responsable de la seguridad de las operaciones electrónicas.
- Implementar procedimientos para la administración de contraseñas en los sistemas de e_commerce, considerar aspectos como caracteres permitidos, cantidad mínima de caracteres, fechas de expiración, número de fallos permitidos y acción frente a las fallas, procesos para cambio de contraseñas entre otros.
- Implementar procedimientos para la emisión de firmas digitales y que sean certificadas por un proveedor externo.
- Mantener un control en las versiones y procedimientos de distribución de software, para las aplicaciones relacionadas con e_commerce.
- Implementar técnicas para monitorear la seguridad de los sistemas e_commerce.
- Desarrollar o adquirir un software que permita realizar análisis de la seguridad.
- Implementar mecanismos para monitorear y detectar intromisiones a la red.
- Implementar un buzón de sugerencias de los usuarios que usan los servicios de e_commerce para que sean considerados en las proyecciones de crecimiento y la planeación.
- Dentro de las normatividades de e_commerce, implementar políticas de seguridad respecto a la encriptación de los datos, definir responsabilidades por mantenimiento, dominios de acceso y reglas que permitan tráfico permitido y prohibido en los cortafuegos (Firewalls).
- Alinear e_commerce con la misión y los planes estratégicos de la entidad.
- Implementar procedimientos para identificar accesos remotos diferentes que el firewall.
- Implementar procedimientos que permita restringir el acceso a la documentación de la configuración del Firewall.
- Implementar procedimientos para prevenir el acceso no autorizado a la red interna.
- Implementar procedimientos para la certificación de pruebas y actualización de las políticas en los cortafuegos.

El procedimiento de Administración de Base de Datos (PT8) tiene un cumplimiento de 44%, debiendo estandarizar las siguientes funciones y/o tareas de acuerdo a las normas técnicas peruanas:

- El administrador de Base de Datos debe tener privilegios a nivel de administrador para hacer cambios a la base de datos.
- Implementar procedimientos para la restructuración de la base de datos, en caso de una destrucción o parcial.
- Registrar en un documento el usuario y clave del DBA lacrado y guardado en lugar seguro.

- Se debe documentar los cambios que se realizan a la Base de Datos.
- Realizar pruebas que permitan prevenir atentados deliberados en la destrucción o modificación en la base de datos, considerando posibles atentados externos como internos.
- Insertar nuevos campos en las tablas de registro de auditoria de la base de datos donde se consideren las acciones de los intentos de conexión, acceso a los objetos y accesos a la base de datos.
- Implementar procedimientos en la que el administrador de base de datos realice acciones con las tablas de registros de auditoria de la base, para corregir fallas o accesos no autorizados.

c. Soporte

En este dominio se evaluará el cumplimiento de los procedimientos de mantenimiento, controles, almacenamiento, seguridad e infraestructura de la Oficina de TI, siendo parte fundamental para la continuidad de las actividades de la entidad.

En el gráfico anterior se puede observar el nivel cumplimiento de los procedimientos del dominio de SOPORTE, siendo el de mayor cumplimiento el de Mantenimiento de Hardware con un 88% (SO1), debiendo complementar las siguientes tareas:

- Realizar un inventariado del hardware que mayor tienden a deteriorarse o malograrse para tener en stock y que puedan ser sustituidas de manera oportuna.
- Mantener un historial respecto a los informes de mantenimiento a nivel físico y de parámetros efectuados a los servidores principales de la entidad.

Otro de los procedimientos de mayor cumplimiento es el de Infraestructura (SO5) con 72%, debiendo complementar las siguientes tareas:

- Coordinar con la Gerencia General, para la elaboración de planos del edificio, con la finalidad de visualizar su distribución para identificar riesgos para el equipo informático.
- Incorporar en el plan anual de mantenimiento de informática, el del falso piso del data center.
- Colocar protección a la caja de suministro de energía, con cerraduras y situarlos en habitaciones o lugares cerrados.
- Colocar lámparas de emergencia en la Oficina de TI, para casos de emergencia.

El procedimiento de Controles de redes y comunicaciones (SO2), tiene un cumplimiento de 63%, está por encima del 50%, es decir tiene un nivel aceptable, debiendo tener en cuenta las siguientes tareas:

- Tener en un sobre lacrado y en un lugar seguro, fuera de la Oficina de TI la clave de los equipos (servidores, proxy, switch), para una eventualidad fortuita.
- Desarrollar procedimientos de autorización para conectar nuevos equipos a la red.
- Implementar procedimientos para el uso de cualquier conexión digital exterior, como línea conmutada o dedicada.
- Documentar reportes de incidencias, contingencias y circunstancia que afecten el funcionamiento de la red, conforme a la bitácora.
- En el servidor de defensa instalar aplicaciones para hacer más seguro el servidor, tales como: Telnet, DNS, FTP, SMTP y autenticación de usuarios, para evitar posibles ataques.
- Dentro del tipo de cable utilizado para el tendido de la red, se recomienda utilizar una categoría superior, actualmente es par trenzado categoría 5e.
- Migración de banda ancha para la salida a internet, actualmente es de 3 Mbps.

El procedimiento de Control de Almacenamiento (SO3), tiene un cumplimiento de 47%, menos del promedio que es 50%; debiendo mejorar en cuenta las siguientes tareas:

- La seguridad donde se almacenan los backups, deben de tener una cerradura de puerta especial (tarjeta electrónica, acceso biométrico, cerradura eléctrica, etc).
- En las cintas de inventariado, complementar la información como: número de serie, número del archivo, detalle del contenido, fecha de expedición del archivo.
- Implementar procesos de encriptamiento y autenticación en el proceso de copiado de la información.
- Realizar periódicamente pruebas de restauración de los medios magnéticos con la finalidad de asegurar la recuperación.
- Desarrollar procedimientos que permita la reconstrucción de un archivo el cual fue inadvertidamente destruido.
- Seleccionar el tipo de información copiado en el medio magnético y si es de carácter confidencial, etiquetarlo como tal.
- Desarrollar un procedimiento que permita tener un control estricto de las copias de archivos de carácter confidencial.
- Certificación de destrucción de dispositivos magnéticos.
- Implementar políticas o medidas de control en caso de extravío de algún dispositivo de almacenamiento.
- Desarrollar procedimientos para el reemplazo o actualización de medios magnéticos de los copias de seguridad.

En este dominio, el procedimiento de menor nivel de cumplimiento es el de Seguridad Física (SO4) con 45%, debiendo tener en cuenta lo siguiente:

- Implementar un sistema de alarma contra incendio automático, debiendo tener la capacidad de transmitir señales a un punto

remoto que sea supervisado las 24 horas. (el punto remoto puede ser una estación de guardia de la organización o la estación de bomberos local).

- Implementar un sistema automático de extinción de fuego en la Oficina de Tecnología de la Información.
- Coordinar capacitaciones para el personal de la Oficina de TI para el uso y manejo de extintores durante un posible incendio y evitar que éste se propague.
- Coordinar con la Gerencia General, para el desarrollo de programas de capacitación para el personal de la entidad, contra incendios y para su evacuación en caso de posible incendio.
- Coordinar reuniones con el personal de seguridad del CGT, e instruirlo respecto a las medidas a tomar en caso de que personal ajeno a la Oficina de TI pretenda ingresar sin autorización.
- Realizar evaluaciones psicológicas respecto a la personalidad de los trabajadores de la Oficina de TI, con el fin de mantener una buena imagen y evitar un posible fraude.

d. Subcontratación

En éste dominio, se evalúa los procedimientos que se realizan entre un proveedor y la entidad, en la adquisición de servicios, recursos informáticos (software y hardware).

En el gráfico anterior se puede observar el cumplimiento de los procedimientos de conforman el dominio de SUBCONTRATACIÓN, siendo el de mayor cumplimiento el de Evaluación del Proveedor (SC2) con un 88%, debiendo complementar las siguientes tareas:

- Durante el proceso de Subcontratación de un proveedor de servicios, identificar si es nacional o internacional, con el objetivo de obtener información sobre: Tipo de representación, ubicación física, personal de enlace, teléfono, etc.

El Procedimiento de Examen de los servicios subcontratados (SC3) tiene un cumplimiento de 83%, debiendo mejorar en las siguientes tareas:

- Designar una persona responsable en la Oficina de TI, que controle de manera permanente la calidad de los productos y/o servicios prestados por el proveedor.
- Evaluar el riesgo de dependencia de la institución hacia el proveedor de servicios y el impacto de éste en las operaciones diarias.
- Realizar un análisis de los riesgo en la subcontratación de servicios, tiendo en cuenta los putos siguientes:
    - Seguridad informática y privacidad de la información de la empresa y de los clientes que implica riesgos legales, normativos y reputación en las jurisdicciones del cliente-anfitrión.

- Los eventos externos (desastres naturales/ disturbios, etc) que restringen la movilidad del personal y el acceso a las instalaciones de procesamiento).

Dentro de éste dominio el procedimiento de menor cumplimiento, pero con promedio aceptable es el de Evaluación de Contratos de Servicios (SC1), teniendo un 53% de cumplimiento, debiendo mejorar en las siguientes tareas:

- Disponer de un archivo, respecto a los contratos de servicios proporcionados por terceros.
- Identificar y realizar un análisis de las condiciones pactadas en cada cláusula de los contratos de prestación de servicios de TI.
- Dentro del contrato de Servicios, deben de considerarse los siguientes condiciones:
    - Medidas de desempeño.
    - Presentación de informes de trabajos realizados.
    - Resolución de diferencias y jurisdicción.
    - Incumplimiento y rescisión.
    - Propiedad y acceso
    - Planificación en caso de contingencia
    - Derechos de Auditoria.
    - Subcontratación o dependencia de otros.
    - Confidencialidad / seguridad/separación de propiedades.
    - Monto de los servicios, objeto del contrato, forma de pago y tipo de moneda.
    - Seguros / Garantías.
    - Ubicación física de la documentación.
    - Revisiones periódicas a los acuerdos.

1.2.3. Organización de las TIC en el Centro de Gestión Tributaria de Chiclayo

a. Estructura organizativa

La Oficina de Tecnologías de Información depende jerárquicamente de la Gerencia General del CGT. Está encargado de un profesional, con categoría de Jefe de Oficina.

De acuerdo al ROF vigente, la Oficina de Tecnología de Información es el órgano de apoyo, encargado de organizar, dirigir, diseñar e integrar e sistema informático del Centro de Gestión Tributaria de Chiclayo. (Aprobado con Ordenanza Municipal N° 009-2015-MPCH y sus modificatorias Ordenanza Municipal N° 018-2016-MPCH/A).

Con la nueva estructura de organizacional de la institución, la Oficina de Tecnología de Información tiene la siguiente estructura orgánica:

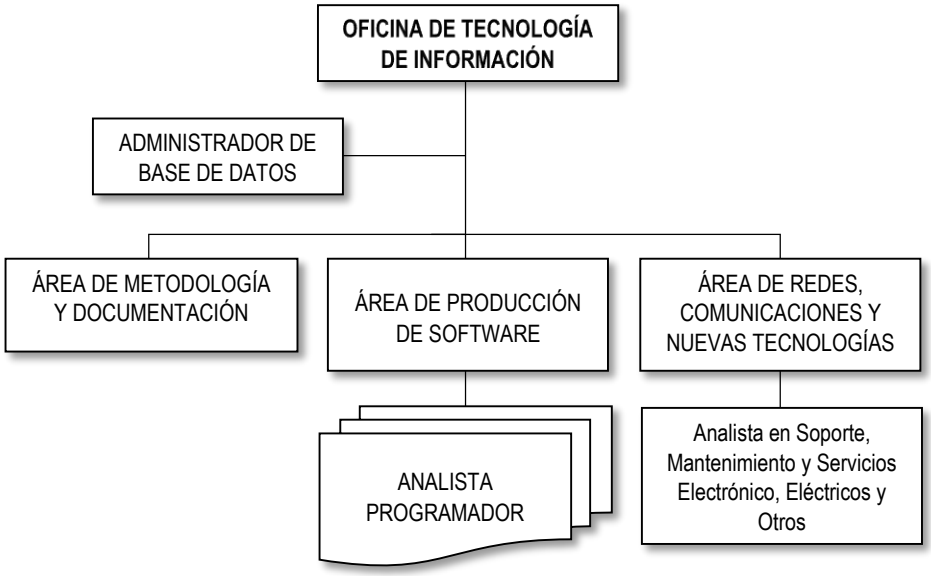


Figura N° 8. Organigrama de la OTI - CGT
Fuente: Plan Estratégico Institucional 2016-2018

Tabla N° 2. Cuadro Orgánico de Cargos de la OTI – CGT

N° de Orden	Denominación	Total Necesario	N° CAP
1	Jefe de la Oficina de Tecnología de Información	1	012
2	Administrador de Base de Datos	1	013
3	Jefe del Área de Metodología y Documentación	1	014
4	Jefe del Área de Producción de Software	1	015
5	Analista Programador	2	016-017
6	Jefe del Área de Redes, Comunicaciones y Nuevas Tecnologías	1	018
7	Analista en Soporte, Mantenimiento y Servicios Electrónico, Eléctricos y Otros.	1	019
TOTAL		8	-

Fuente: Manual de organización y funciones del Centro de Gestión Tributaria de Chiclayo (CGT Chiclayo, 2018)

b. Sistemas de Información

En el mapa de sistemas de información del Centro de Gestión Tributaria de Chiclayo, se ha clasificado de la siguiente manera:

- Por tipo de desarrollo: Que ha sido desarrollado en la OTI (propio) y desarrollados o adquirido por terceros.
- Por entorno del sistema: Sistema desarrollado en entorno web o desarrollado en entorno de escritorio.

Figura N° 9. Mapa de sistemas de información OTI - CGT
Fuente: Elaboración propia

Tabla N° 3. Fichas Técnicas de Sistemas y Aplicativos

Nombre de Sistema	Software de Tributación Municipal
Nombre Corto	STM
Módulos	Registro, Fiscalización, Licencias, Tesorería, Cobranzas, Coactiva, Consultas, Estadísticas, Herramientas, Administrar sistema, Mantenimiento.
Descripción	Este es el principal aplicativo informático de la institución. Tiene módulos por cada uno de los tributos para el proceso de registro de información, cálculo de Impuesto predial, cálculo de arbitrios, transferencia de predios, registro de pagos, gestión de cobranza ordinaria, gestión de cobranza coactiva y levantamiento catastral, Módulos de Otros Ingresos (Merced Conductiva, etc.). Así mismo cuenta con módulos para consultas y módulos para estadísticas
Información que registra	Registro de Contribuyentes, Registro de Predios, Registro de Vehículos, Cálculos de Impuesto Predial, Calculo de arbitrios municipales, Transferencia de Predios, Registro de Licencias de Funcionamiento, registro de papeletas de tránsito y papeletas administrativas, deudas de contribuyentes, pagos realizados por contribuyentes, cierres de caja, etc.
Áreas Usuarias	Todas las áreas del CGT
Área Propietaria	Gerencia de Operaciones
Registrado en Indecopi	Sí
Lenguaje de Programación	Microsoft Visual Basic 6.0
Cuenta con Códigos Fuente	Sí
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Cliente / Servidor
Tiempo que está en Producción	Desde el 2005
Responsable del Mantenimiento	Unidad de Desarrollo de Sistemas

Nombre de Sistema	Programa de Administración de Documentos
Nombre Corto	PAD
Módulos	Inicio, Tramitación, Consultas, Reportes, Herramientas y Seguridad.
Descripción	Aplicativo desarrollado para la recepción y control de los expedientes tramitados por los contribuyentes. Este sistema posee módulos para el registro de los diferentes formatos de trámites realizados por los contribuyentes y para el registro de los diferentes movimientos entre las diferentes áreas del CGT.
Información que registra	Registro de Expedientes por tipo de trámite y es derivado de manera sistemática a la unidad correspondiente para su atención.
Áreas Usuarias	Todas las áreas del CGT
Área Propietaria	Gerencia de Operaciones

Registrado en Indecopi	Sí
Lenguaje de Programación	Microsoft Visual Studio Professional 2012
Cuenta con Códigos Fuente	Sí
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Cliente / Servidor
Tiempo que está en Producción	Desde el 2010
Responsable del Mantenimiento	Unidad de Desarrollo de Sistemas

Nombre de Sistema	Programa de Administrativo del CGT
Nombre Corto	PAS
Módulos	Personal, Presupuesto, Contabilidad, Logística, Tesorería, Centro de Costo, Consultas y Seguridad
Descripción	Software utilizado por las áreas administrativas del CGT. Posee módulos para el control y administración de la información tanto de Personal, Planificación, Control Presupuestal, Logística, Contabilidad y Tesorería.
Información que registra	Registro de trabajadores, registro de planillas, registro de proveedores, registro de requerimientos de bienes activos y no activos, generación de Orden de compra, generación de orden de servicio, registro de afectaciones presupuestales, registro de asientos contables, registro de comprobantes de pago, etc
Áreas Usuarias	Todas las áreas del CGT
Área Propietaria	Gerencia de Administración
Registrado en Indecopi	Sí
Lenguaje de Programación	Microsoft Visual Studio Professional 2012
Cuenta con Códigos Fuente	Sí
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Cliente / Servidor
Tiempo que está en Producción	Desde el 2012
Responsable del Mantenimiento	Unidad de Desarrollo de Sistemas

Nombre de Sistema	Sistema de Control de Colas CC+
Nombre Corto	-
Módulos	Edición, Administrador, Consultas, Herramientas y Ayuda
Descripción	Aplicativo que sirve para generar tickets de atención a contribuyentes. Permite mostrar y visualizar videos y banners cargados por personal de la institución
Información que registra	Generación de tickets de atención, Registro de videos, etc.
Áreas Usuarias	Dpto. de Registro
Área Propietaria	Registro
Registrado en Indecopi	-

Lenguaje de Programación	Visual FOX
Cuenta con Códigos Fuente	No
Gestor de base de datos	DbaMGR2k
Indicar si es: Web / Cliente Servidor	Cliente / Servidor
Tiempo que está en Producción	Desde el 2008
Responsable del Mantenimiento	-

Nombre de Sistema	Sistema de Saldomático
Nombre Corto	
Módulos	Consultas Predial, Arbitrios, Vehicular y Papeletas
Descripción	Este aplicativo emite y muestra información sobre el estado de cuenta a todos los contribuyentes que se encuentren registrados en las bases de datos de la institución y que tienen deuda por: Impuesto predial, Impuesto vehicular, Arbitrios municipales y Papeletas de tránsito.
Información que registra	Emite información de deudas por Impuesto predial, Impuesto vehicular, Arbitrios municipales y Papeletas de tránsito de los contribuyentes registrado en la base de datos del CGT.
Áreas Usuarias	Contribuyentes
Área Propietaria	Tesorería
Registrado en Indecopi	No
Lenguaje de Programación	Java
Cuenta con Códigos Fuente	Sí
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Web
Tiempo que está en Producción	Desde el 2010
Responsable del Mantenimiento	-

Nombre de Sistema	Sistema de Control de Ingreso a parqueo vehicular
Nombre Corto	SCIPV
Módulos	Inicio, Entrada, Salida, Reportes y Mantenimiento
Descripción	Aplicativo que permite registrar y controlar el acceso (ingreso y salida) de vehículos menores y de mayor capacidad a la chochera municipal de la Av. Balta
Información que registra	Información de sedes, puertas, usuarios, ingreso y salida de las placas de vehículos
Áreas Usuarias	Otros Ingresos - Parqueo
Área Propietaria	Cobranzas
Registrado en Indecopi	-
Lenguaje de Programación	PHP
Cuenta con Códigos Fuente	Si
Gestor de base de datos	MySQL

Indicar si es: Web / Cliente Servidor	Web
Tiempo que está en Producción	Desde el 2011
Responsable del Mantenimiento	-

Nombre de Sistema	Sistema de Atención al Usuario
Nombre Corto	SATUS
Módulos	Inicio, Formatos Internos, Registrar Papeleta, Buscar Papeleta, Información, Cambiar Clave, Manual de Usuario y Cerrar Sesión.
Descripción	Sistema utilizado para gestionar las salidas del personal del CGT mediante el registro y autorización de papeletas de salida.
Información que registra	Registra la hora de salida y regreso del personal del CGT , el tipo de salida, Lugar de destino y Motivo de salida; estas autorizaciones se realiza por jerarquía.
Áreas Usuarias	Todas las áreas del CGT
Área Propietaria	Departamento de Recursos Humanos
Registrado en Indecopi	No
Lenguaje de Programación	PHP
Cuenta con Códigos Fuente	Si
Gestor de base de datos	Postgres
Indicar si es: Web / Cliente Servidor	Web
Tiempo que está en Producción	
Responsable del Mantenimiento	-

Nombre de Sistema	AutoStor
Nombre Corto	
Módulos	Inicio, configuración de Ordenamiento
Descripción	Aplicativo utilizado para la digitalización de Papeletas de Tránsito mediante la lectura de código de barras
Información que registra	Escaneo de las papeletas de tránsito, guardados en formato pdf para consultas en el módulo de registro de papeletas del STM.
Áreas Usuarias	Emisiones
Área Propietaria	Cobranzas
Registrado en Indecopi	NO
Lenguaje de Programación	Windows Server 2003 R2 Standard Edition SP2
Cuenta con Códigos Fuente	No
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Cliente/ Servidor
Tiempo que está en Producción	
Responsable del Mantenimiento	

Nombre de Sistema	Bioidentidad BioStar v1.61
Nombre Corto	
Módulos	Inicio, Registro de Personal, Registro de Huella dactilar de cada persona, Ingreso de Horarios ,Imagen,Asignación de horarios, Reportes General por día, Reportes por Personal por mes,
Descripción	Permite que llevar el Control de Asistencia y Permanencia del personal en el CGT durante su jornada laboral a través del marcado con huella dactilar
Información que registra	Registra la hora de ingreso y salida del pesonal, así como la salida e ingreso de refrigerio del personal.
Áreas Usuarias	Todas las áreas del CGT
Área Propietaria	Departamento de Recursos Humanos
Registrado en Indecopi	Si
Lenguaje de Programación	Visual FOX
Cuenta con Códigos Fuente	Si
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Cliente/ Servidor
Tiempo que está en Producción	
Responsable del Mantenimiento	

Nombre de Sistema	Portal Institucional
Nombre Corto	
Módulos	Página Principal, Portal de Transparencia, Consultas en Línea, Correo Institucional, Consultas de Contribuyente, mapa web.
Descripción	Se encuentra información referente a la Institución, estadísticas, de recaudación, consultas de en línea (de expedientes, de deuda tributaria, Record de infracciones).
Información que registra	-
Áreas Usuarias	Administrados y público en general
Área Propietaria	Oficina de Tecnologías de la Información
Registrado en Indecopi	
Lenguaje de Programación	PHP
Cuenta con Códigos Fuente	Si
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Web
Tiempo que está en Producción	
Responsable del Mantenimiento	

Nombre de Sistema	Intranet
Nombre Corto	
Módulos	Inicio, Información de la Institución, Áreas de Institución, Personal, Normatividad y Ordenanzas, Misceláneos, EducaCGT, páginas de Interés.
Descripción	Se encuentra información referente a la institución, Directorio Telefónico, Relación de personal con sus respectivos cargos, documentos internos, relación de vacaciones, así como relación de páginas de interés a las que pueden ingresar el personal de manera predeterminada.
Información que registra	
Áreas Usuarias	Personal que labora en el CGT
Área Propietaria	Oficina de Tecnologías de la Información
Registrado en Indecopi	-
Lenguaje de Programación	PHP
Cuenta con Códigos Fuente	Si
Gestor de base de datos	Microsoft SQL Server 2008
Indicar si es: Web / Cliente Servidor	Web
Tiempo que está en Producción	
Responsable del Mantenimiento	Área de Producción de Software

Del análisis de los Sistemas de Información se tiene la siguiente estadística:

Tipo de Desarrollo	N° de Sistemas
Propio	6
Terceros	5
Total general	**11**

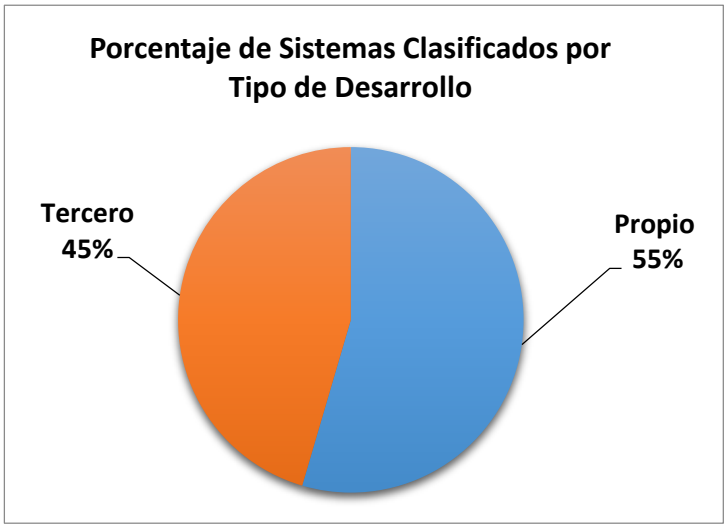


Figura N° 10. Porcentaje de Sistemas clasificados por tipo de desarrollo OTI - CGT
Fuente: Elaboración propia

Del cuadro y gráfico anterior, se observa que 55% de los sistemas han sido desarrollados por el personal de la Oficina de Tecnologías de Información del Centro de Gestión Tributaria de Chiclayo.

c. Plataforma Tecnológica

Arquitectura de Comunicaciones

El Centro de Gestión Tributaria de Chiclayo, actualmente cuenta con un DATA CENTER ubicado en la Oficina de Tecnologías de Información, que se ha venido implementando de acuerdo a las necesidades de seguridad de la institución.

El soporte y mantenimiento está a cargo del personal del Área de Redes, Comunicaciones y Nuevas Tecnologías, como se mencionó anteriormente la infraestructura tecnológica del CGT se ha incrementado, pero el personal de ésta área sigue siendo los mismos en número, en varias ocasiones no se alcanzan a cubrir todos los requerimientos solicitados por las diferentes unidades orgánicas del CGT.

Acceso a Internet

En el Centro de Gestión Tributaria se cuenta con acceso a Internet con ancho de banda de 3 Mbps, cuyo proveedor es Movistar.

Red LAN y Cableado Estructurado

En la sede principal del Centro de Gestión Tributaria de Chiclayo se conectan los equipos a través de cable estructurado UTP categoría 5e y a través de antenas con sus locales desconcentrados formando una RED LAN en topología Estrella Jerárquica.

La red de distribución corren a una velocidad de 10/100 Mbps a nivel de puesto de trabajo.

El cableado del Backbone es de tipo UTP, e interconecta de manera vertical a los equipos distribuidos de las oficinas en los pisos.

Inventario de Software

En el Centro de Gestión Tributaria de Chiclayo se cuenta con diversos tipos de software tanto libre como con licencia, para el cual se ha clasificado en 3 grupos:

- **Software de Sistema:** permite a los usuarios interactuar con el sistema operativo así como también controlarlo.

Tabla N° 4. Inventario de software de sistema

Cant. Lic.	Licencia	Soft. Libre	Tipo
63	Windows 7 Profesional		Sistema Operativo
35	Windows XP Pro SP3		Sistema Operativo
29	Windows 7 Pro - Downgrade a XP		Sistema Operativo
21	Windows 8 Profesional		Sistema Operativo
2	CentOS Linux 4.2		Sistema Operativo
2	Windows Server 2003 R2		Sistema Operativo
1	Gentoo Linux		Sistema Operativo
1	Ubuntu Server		Sistema Operativo
1	TEMPRECORD – TRW V5.28.0 Build 2471_11July2012		Utilitario
1	Srvtouch		
	Vncviewer	si	Utilitario

- **Software de Aplicación:** software diseñado para el usuario final, aquellos programas que permiten al usuario realizar una o varias tareas específicas día a día.

Tabla N° 5. Inventario de software de aplicación

Cant. Lic.	Licencia	Soft. Libre	Tipo
1	VLC Media Player	si	Audio
	Google Chrome	si	Buscador
	SetupDWGTrueView2016_ ENU_32bit.sfx	si	CAD
	DWG True View 2009	si	CAD
	GoogleEarthProSetup	si	Cartografía
	Windows Mail	si	Correo
1	Lightshot-4.4.2.10	si	Diseño
	CDRViewer	si	Diseño
145	Open Office 4.1.2	si	Oficina
	PDF Creator	si	Oficina
	Adobe Reader 9	si	Oficina
	Install SIMI3.5 (Limitado)	si	Sistema-Estado
	PDT Planilla Electrónica	si	Sistema-Estado
50	ESET Endpoint Protection Standard		Antivirus
7	Consultas Reniec en Línea		Aplicación del Estado
1	Quick Capture Desktop		Captura de Imagen
1	ZEBRA Designer Pro		Código de Barras
1	Corel DRAW Graphics Suite X8 License ML GOV		Diseño

30	Office Hogar y Pequeña Empresa 2013		Oficina
26	Office Hogar y Pequeña Empresa 2010		Oficina
6	Microsoft Office H&B 2016		Oficina
2	Canon DR-2080C Scanner Driver		Oficina
1	Hp Storage Works Data Protector Express		Oficina
	Adobe Reader 9.1 Español		Oficina
1	Vivotek ST3402		Seguridad-Cámaras
1	BioStar		Seguridad Digital
1	Class Colas (Application Proxy)		Sistema-Interno
1	Clic llamada C++		Sistema-Interno
1	colasadmi		Sistema-Interno
1	Sist. Parqueo y Tranquera		Sistema-Interno
	PAS (Limitado)		Sistema-Interno
	STM (Limitado)		Sistema-Interno
	PAD (Limitado)		Sistema-Interno
	Sigmu (Limitado)		Sistema-Interno
	Sismant (Limitado)		Sistema-Interno
1	Correccion Digit		
1	AutostoreWF		

- **Software de Programación**: que ayuda en la creación y desarrollo de aplicaciones, haciendo uso de conocimientos lógicos y de programación.

Tabla N° 6. Inventario de software de programación

Cant. Lic.	Licencia	Soft. Libre	Tipo
1	Microsoft SQL Server 2012		Base de Datos
1	SAP Crystal Reports		Desarrollo
1	Microsoft Visual Studio Professional 2012		Desarrollo

Inventario de Hardware

Se realizó un inventario del hardware del CGT, en los que se llevan a cabo el desarrollo de las labores del todo el personal.

- **Servidores**
  El CTG cuenta con un total de 12 servidores, instalados en el Data Center de la Oficina de Tecnologías de Información.

Servidores por Tipo de Fabricante	Cantidad
Compatible	5
DELL	1
HP	4
IBM	2
Total general	**12**

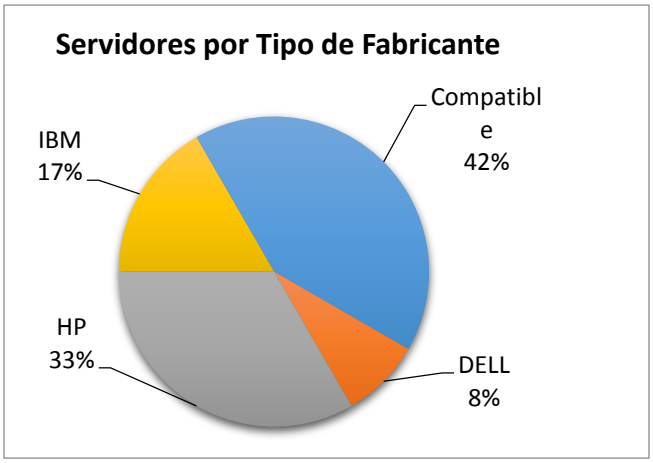


Figura N° 11. Porcentaje de servidores por tipo de fabricante en la OTI - CGT
Fuente: Elaboración propia

En el cuadro y gráfico anterior se puede observar que 5 de los 12 servidores son COMPATIBLES, es decir computadoras de escritorio adaptadas para que funcionen como Servidores.

Debemos tener en cuenta que un servidor está diseñado para trabajar de forma continuada, normalmente sin ser apagado, es decir las 24 horas del día, los 7 días de la semana, durante los 365 días del año.

Así mismo los servidores tienen características funcionales de:

- Alto Rendimiento: Cuentan con discos duros internos de mayor velocidad (10k/15k rpm) a diferencia de los equipos de escritorio (5k-10k rpm) o bien con conexiones a para redes de áreas de almacenamiento (Storage Área Networks - SAN) que pueden tener varios discos de alta velocidad trabajando de manera simultánea y transmitiendo información a través de la red, lo que reduce drásticamente los tiempos de respuesta.

  Además en servidores, es común encontrar CPUs con características especiales de alto desempeño, que permiten ejecutar varias instrucciones simultáneamente, entre otras, capacidades no encontradas en los equipos de escritorio.

- Alta Disponibilidad: En segundo lugar, y tal vez más importante, es que los servidores cuentan con capacidades de alta disponibilidad, es decir que son capaces de estar activos mucho más tiempo que los equipos normales.

Una de estas características es la redundancia de hardware, es decir, estos equipos suele contar con discos duros redundantes (usualmente ligados a tarjetas RAID), fuentes de poder redundantes, canales de comunicación duales (en tarjetas de red o fibras ópticas) lo cual hace menos probable que se tenga un downtime (falta de tiempo) debido a fallas de hardware. Además el acceso a discos externos vía SAN (Red de Áreas de Almacenamiento) suele tener redundancia por sí mismo, de manera que si algún disco falla, otro disco suele entrar como backup lo que minimiza la posibilidad de pérdida de información.

Además suelen venir equipados con memoria ECC (Error Correcting Code) que previene en ciertos casos la corrupción de datos en memoria.

Tabla N° 7. Año de Fabricación de Procesadores de Data Center del CGT

Tipos de Procesadores por Servidor	Cuenta de Procesador	Año de Fabricación (Fuente Intel)	%
AMD phenom II X4 965	1	2008	8%
Inte Core2 Quad Q9550	1	2008	8%
Intel Celeron	1	1998	8%
Intel Pentium IV	3	2002	25%
Intel Xeon E3-1200 v3	1	2013	8%
Intel Xeon E5-2650	1	2012	8%
Intel Xeon E5-2650 v2	1	2013	8%
Intel Xeon E5320	1	2006	8%
Intel Xeon E5345	2	2007	17%
Total general	**12**	-	100%

El gráfica y cuadro anterior, se puede observar que el 33% delos servidores son de tecnología de más de 14 años, es decir necesitan de ser reemplazadas; las mismas que en la actualidad las empresas fabricantes de los procesadores ya no dan soporte.

Tabla N° 8. Equipos de cómputo del usuario final por tipo de procesador

Tipo de Procesador	N° de PCs	Año de Lanzamiento (Fuente Intel)
AMD PHENOM II X4	28	2008
Intel Atom D-525 / 1M /1.8 Ghz Dual Core	1	2010
INTEL CORE 2 DUO	19	2008
INTEL CORE I3	1	2010
INTEL CORE I5	20	2012
INTEL COREI7	9	2013
INTEL DUAL CORE	30	2007
INTEL PENTIUM IV	16	2004
(en blanco)	16	-
Total general	**140**	**-**

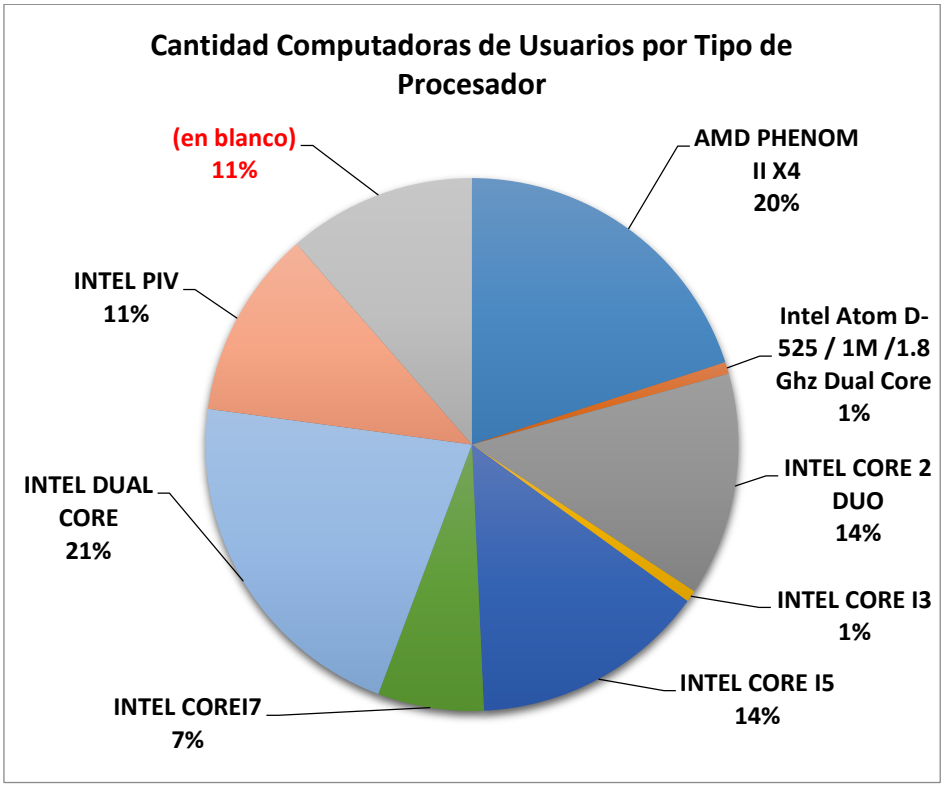


Figura N° 12. Porcentaje de servidores por tipo de fabricante en la OTI - CGT
Fuente: Elaboración propia

Tabla N° 9. Equipos de cómputo del usuario final por sistema operativo

Sistema Operativo	N° de Pcs
Windows 7 Pro - Downgrade a XP	28
Windows 7 Profesional	3
Windows 7 Profesional - 64 bits	17
Windows 7 Profesional 32bits SP1	3
Windows 8 Profesional	24
Windows XP SP3	36
(en blanco)	29
Total general	**140**

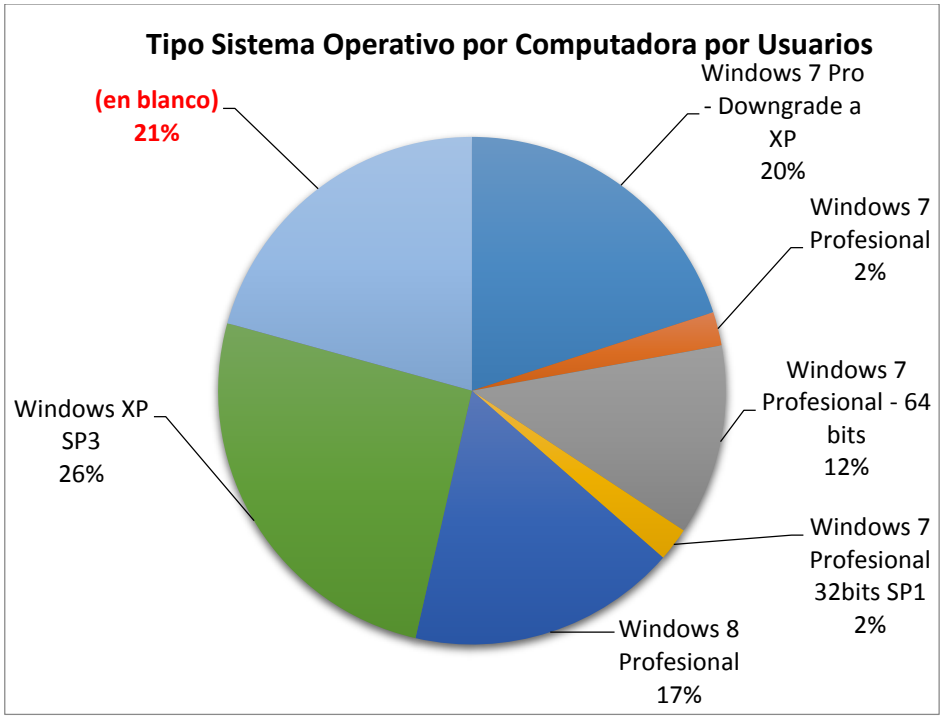


Figura N° 13. Porcentaje de servidores por tipo de fabricante en la OTI - CGT
Fuente: Elaboración propia

- **Computadoras Portátiles**
  Realizando un análisis de las computadoras portátiles, se cuenta con 2 equipos portátiles, y cuentan con procesador Core I7 cuyo de año de fabricación es del año 2013.

Tabla N° 10. Inventario de computadoras portátiles

Tipo de Procesador	N° de PCs	Año de Lanzamiento (Fuente Intel)
INTEL CORE I7	2	2013

- **Impresoras**

  Del inventario de las impresoras, se puede observar en el gráfico:

  - Que el 45% de las impresoras de tipo laser, que son mayormente usadas para la impresión de documentos internos de cada unidad orgánica.
  - El 32% son de tipo matricial, usada para la impresión en su mayoría en los terminalistas de caja para la entrega del Boucher por la cancelación de sus tributos o tasas administrativas.
  - El 15% son de tipo laser/multifuncional , que adicionalmente son usadas para el escaneo de documentos críticos de cada unidad orgánica.
  - 7% son de tipo térmica, usadas para la consultas de los administrados en el saldomático y en la impresión de códigos de barras para la digitalización de las multas de tránsito.
  - El 1% de tipo inyección, usada por el personal de Imagen institucional para la impresión de diseños artísticos, respecto a volantes de vencimientos de la deuda tributaria, beneficios tributarios y no tributarios, etc.

Tabla N° 11. Inventario de impresoras por tipo en el CGT

Tipo de Impresora	N° de Impresoras
Inyección	1
Laser	27
Laser/multifuncional	9
Matricial	19
Térmica	4
Total general	**60**

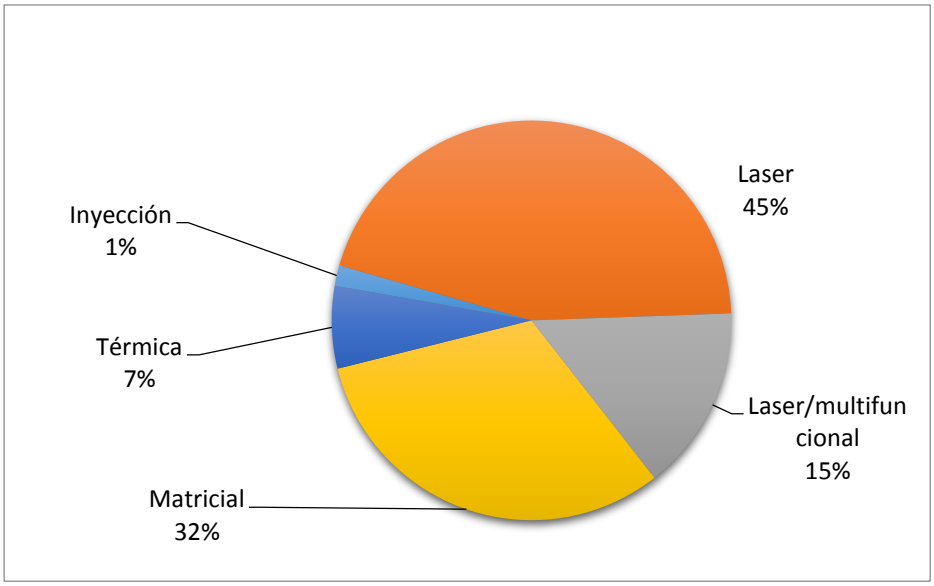


Figura N° 14. Total de impresoras por tipo en la OTI - CGT
Fuente: Elaboración propia

1.2.4. Diagnóstico de la Situación Actual de la Arquitectura Tecnológica

De acuerdo a la información analizada, se puede se concluye en lo siguiente para la mejora de las actividades que se desarrollan en la entidad:

- Se debe evaluar y desarrollar un Proyecto de renovación de Servidores, que permitan dar soporte a las sistemas y programas que se usados para el desarrollo de las actividades de la entidad.
- Que en el Procedimiento PO2 (Plan de Contingencia), se debe desarrollar un plan para la implementación de un servidor de contingencia para todas las aplicaciones y datos críticos.
- Se requiere evaluar y desarrollar un Plan de adquisición de infraestructura tecnológica (hardware, software y comunicaciones), que permitan el desarrollo de los procedimientos de las unidades orgánicas.
- Migración a un de ancho de banda mayor a 3 Mbps, el actual ancho de banda se satura por el crecimiento de la red de datos.
- Respecto al Procedimiento PT9 (Seguridad lógica), se debe adquirir equipos que puedan validar la identificación electrónica de las terminales que se agregan a la red.
- La evaluación de un plan para la adquisición de herramientas para monitorear y detectar intromisiones a la red y así como un software para el análisis de seguridad, de acuerdo al procedimiento PT10 (Comercio electrónico) del dominio de Plataforma Tecnológica.
- Aumento de las ocurrencias de incidencias relacionadas con la seguridad informática y la seguridad de la información.

- No existen políticas, ni procedimientos ni normativas que estén relacionadas con la seguridad y la gestión de riesgos.
- A pesar de que cuentan con un inventario de los activos tecnológicos no se ha definido ni priorizado que activos son los más importantes ni la relación que existen con los procesos de la Oficina de TI, ocasionando que la información no sea fiable o no esté disponible en el momento oportuno.
- La Oficina de TI no cuenta con un proceso de evaluación y de tratamiento de riesgos, para poder analizar de manera apropiada las amenazas, vulnerabilidades e impacto relacionados con cada activo generando que aumente el impacto negativo sobre la seguridad de la información.
- Así mismo no se cuenta con seguridad de los mismos equipos para evitar la pérdida, daño o robo de los activos tecnológicos pudiendo generar interrupciones de las actividades de la misma entidad.
- Hasta el año pasado contaban con un documento que registraba las incidencias y la atención de problemas, sobre todo de aquellos problemas técnicos los cuales son los más comunes en el CGT sin embargo este proceso no contaba con un adecuado procedimiento por lo que este año, este documento no se está utilizando ocasionando falta de atención oportuna de incidencias y atención de esos problemas, aumentando potencialmente sus impactos negativos sobre la seguridad de la información.
- Los procesos de soporte técnico y el de administración de redes y comunicaciones no están debidamente documentados generando en ocasiones fallos, interrupciones e incertidumbre al momento que ocurre un problema al no saber qué proceso seguir para poder solucionarlo.
- No existe una correcta segregación de los deberes y funciones dentro de la Oficina de TI.
- A pesar que si existe un respaldo de back-up de la información de los sistemas, éste no cuenta con políticas de copias de respaldo de información.
- No hay una correcta gestión de seguridad en la administración de la red en el CGT esto porque no existen controles de redes o no existen políticas sobre el uso de servicios de la red generando problemas en su seguridad y fallos de conexión.
- A pesar de que la información pública está disponible en internet no existe un control que proteja su integridad para evitar una modificación no-autorizada.
- No existen un procedimiento formal para el registro y des-registro del usuario ocasionando que haya problemas al otorgarle y revocarle el acceso a los sistemas y servicios de información que necesita.
- No existe procedimientos, políticas ni normas que eviten el acceso de usuarios no –autorizados, ni tampoco existe un procedimiento para una correcta identificación y autentificación del usuario a los sistemas, poniendo en peligro la información, y así ocasionar un robo de información de los medios de procesamiento de la información.

- Existen algunas inconsistencias en la información de algunos sistemas que emplea el CGT como con el sistema de predios que utilizan y esto porque los mismos usuarios ingresan de manera errónea la información generando problemas de integridad de esta.
- Un notorio problema es la falta de documentación de algunos sistemas que el CGT utiliza, y en otros sistemas esta documentación está muy desfasada generando incertidumbre al no saber cómo poder solucionar ciertos problemas que se presentan en estos.

1.3. Descripción de la Seguridad de la Información del CGT.

Para realizar una descripción más detallada a todo el CGT en lo relacionado a seguridad de la información utilizaremos la norma NTP ISO 27002:2005 para clasificar los hallazgos encontrados en base a sus 11 dominios y a los controles que establece esta norma. Así mismo se determinarán las consecuencias por aquellos controles que no se cumplen y también se tomara en cuenta la efectividad de cada control en base al cumplimiento de la declaración de aplicabilidad (SOA) de esta norma.

A. Política de Seguridad

a. Hallazgos:

En este aspecto el CGT no cuenta con documentos de políticas de Seguridad de la Información, a pesar de que se realizan algunos procedimientos relativos a la seguridad de la Información, estos no se encuentran normados ni documentados

b. Consecuencias:

Al no contar con políticas de seguridad, la información y los activos del CGT no se previenen ni gestionan los daños que se originarían si alguna vulnerabilidad a los cuales está en constante riesgos, explote.

c. Cumplimiento del SOA:

Tabla N° 12. Cumplimiento del dominio de Política de Seguridad

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Política de Seguridad	5.1	Política de seguridad de la información				
	5.1.1	Documento de política de seguridad de la información			✓	
	5.1.2	Revisión de la política de seguridad de la información			✓	

Fuente: Elaboración propia

B. Organización de la Seguridad de la Información.

a. Hallazgos:

No se establece en el CGT una estructura de gestión que controle la implantación de la seguridad de la información, no existe un compromiso claro por parte de la gerencia en estos aspectos, si bien el personal de la Oficina de TI tienen cierto conocimiento sobre estos temas no se les asignado claramente sus responsabilidades sobre seguridad de la información, como tampoco existen acuerdos de confidencialidad debidamente normados y procedimentados para la protección de información.

No se tiene establecido controles de seguridad en contratos realizados a terceros, ni una evaluación del riesgo para determinar sus implicaciones de seguridad y las medidas de control que requieren.

De la revisión de las funciones asignadas a cada puesto de trabajo de la Oficina de TI se encontró que no hay funciones asignadas relacionadas con la seguridad de la información.

b. Consecuencias:

Al no definir y asignar responsabilidades de seguridad, puede ocurrir que cuando la seguridad sea atacada, el usuario de TI que cometa un error busca un culpable y quedar libre de todo cargo, es por ello que se deben asignar claramente responsabilidades para que cuando se den los problemas, cada quien responda por sus actos y por lo que estaba bajo su cargo.

Al no contar con acuerdos de confidencialidad bien establecidos, la información organizacional del CGT podría usarse de manera irresponsable o acceder a ella y luego ser divulgada sin autorización.

Al no tener un especial cuidado con respecto a los contratos que el CGT haga con terceros, la seguridad de la información puede verse afectada.

c. Cumplimiento del SOA

Tabla N° 13. Cumplimiento del dominio de Organización de la seguridad de la información

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Aspectos Organizativos de la SI	6.1	Organización Interna				
	6.1.1	Compromiso de la Dirección con la seguridad de la información.		X		
	6.1.2	Coordinación de la seguridad de la información.			X	
	6.1.3	Asignación de responsabilidades relativas a la seguridad de la información.			X	
	6.1.4	Proceso de autorización de recursos para el tratamiento de la información.			X	
	6.1.5	Acuerdos de confidencialidad.		X		
	6.1.6	Contacto con las autoridades.		X		
	6.1.7	Contacto con grupos de especial interés.			X	
	6.1.8	Revisión independiente de la seguridad de la información			X	
	6.2	Seguridad en los accesos de terceras partes				
	6.2.1	Identificación de los riesgos derivados del acceso de terceros.			X	
	6.2.2	Tratamiento de la seguridad en la relación con los clientes.			X	
	6.2.3	Tratamiento de la seguridad en contratos con terceros.			X	

Fuente: Elaboración propia

C. Gestión de Activos

a. Hallazgos:

Se puede evidenciar que actualmente el CGT no cuenta con una política formalmente establecida en la cual exija inventariar los activos de información; sin embargo si se tiene un inventario actualizado.

En cuanto al inventario realizado por el personal de la Oficina de Tecnología de la Información, este se encuentra implementado en una hoja de cálculo (Excel), pero ya cuentan con una aplicación web desarrollado por ellos mismos. Esta aplicación esta ya concluida pero está en etapa de prueba, y también ya están trasladando toda la información de la hoja de cálculo a este software para su posterior funcionamiento, sin embargo este sistema no tiene implementado una clasificación de sus activos en la cual indique el grado de criticidad del activo, ya que algunos elemento de información pueden requerir un nivel adicional de protección o un uso especial.

b. Consecuencias:

Al no contar con una política en la cual exija inventariar los activos de información, se podría más adelante contar con un inventario desactualizado y así generar inexactitudes en el análisis de los riesgos de TI, lo cual puede incidir en la seguridad de información y si ya se encuentra implementado el SGSI propuesto afectar en la eficacia de este.

Al no establecer una clasificación a los activos de información no podemos indicar la necesidad, prioridad y grado de protección que este necesita.

c. Cumplimiento del SOA

Tabla N° 14. Cumplimiento del dominio de Gestión de Activos

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Clasificación y Control de Activos	7.1	Responsabilidad sobre los activos.				
	7.1.1	Inventario de activos.	X			
	7.1.2	Propiedad de los activos.		X		
	7.1.3	Uso aceptable de los activos.			X	
	7.2	Clasificación de la información.				
	7.2.1	Directrices de clasificación.		X		
	7.2.2	Etiquetado y manipulado de la información.			X	

Fuente: Elaboración propia

D. Seguridad de los Recursos Humanos

a. Hallazgos

Como parte de la contratación en el CGT, el personal y terceros aceptan y firman los términos y condiciones del contrato de

empleo (ya sea temporal o de larga duración), el cual establece sus obligaciones y las obligaciones del CGT, pero no existe una inclusión de la seguridad de la información en sus obligaciones y funciones laborales como tampoco reciben capacitaciones en cuanto a estos temas.

Así mismo la selección de personal lo realiza la Unidad de Recursos Humanos, siguiendo una serie de políticas y procedimientos.

Base legal sujeta a estos procedimientos tenemos:

- Ley Nº 27444, Ley de Procedimientos Administrativos General
- Ley de Presupuesto del Sector Público para el Año Fiscal 2018.
- Ley Nº 27050
- Ley General de la Persona con Discapacidad
- Decreto Legislativo Nº 1057, Régimen Especial de Contratación Administrativa de Servicios.
- Decreto Supremo Nº 075-2008-PCM, Reglamento del Decreto Legislativo Nº 1057.
- Decreto Supremo Nº 065-2011-PCM, modifica el Reglamento del Decreto Legislativo Nº 1057.
- Ley N° 29849, Ley que Establece la eliminación Progresiva del Régimen Especial del Decreto
- Legislativo N° 1057 y Otorga Derechos Laborales.

Tipos de contratos de personal sujeta al CGT son:

- Contratación Administrativa de Servicios (Cas):
  El personal presta un servicio no autónomo, subordinado y dependiente dentro de las instalaciones del CGT, la selección se llevará a cabo en forma pública, en la que tendrán la opción de postular todos los ciudadanos que reúnan los siguientes requisitos:

- Contrato por Locación de Servicios
  El personal que es contratado para desempeñar un servicio especializado, con un resultado pre-definido y en cuyo caso el contratado deberá aportar los materiales y elementos de trabajo.

  En ambas los postulantes al servicio convocado, serán evaluados en los siguientes factores de selección:

  a) Evaluación Curricular: En esta fase se evaluará el nivel educativo y académico alcanzado por los postulantes, además de su experiencia laboral afín con el servicio al que postula.

  b) Entrevista Personal: Se realizará con la finalidad de que se conozca al postulante, su grado de cultura general y predisposición para la prestación del servicio.

Así mismo existe una Resolución de Designación.

b. Consecuencias

Si los empleados, contratistas y terceros no están al tanto de sus responsabilidades de seguridad podríamos aumentar el riesgo a hurto, fraude o mal uso de las instalaciones del CGT.

La mala gestión que atraviesa el CGT puede causar al personal sentirse infravalorado resultando en un impacto negativo en la seguridad de la organización, esto puede llevar a que la seguridad de la información sea descuidada o utilizar de forma inadecuada los activos del CGT.

Al no recibir un entrenamiento apropiado en cuanto a la concientización y capacitación en seguridad de la información el CGT correrá riesgos de no adopción de los usuarios a la política de seguridad de información implantada y a otras políticas y prácticas derivadas. Así mismo el personal no se sentirá motivado con estos temas y podría generan más incidentes que perjudiquen la seguridad de información.

c. Cumplimiento del SOA

Tabla N° 15. Cumplimiento del dominio de Seguridad en RRHH

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Seguridad en Recursos Humanos	8.1	Seguridad antes del empleo.				
	8.1.1	Funciones y responsabilidades.		X		
	8.1.2	Investigación de antecedentes.	X			
	8.1.3	Términos y condiciones de contratación.	X			
	8.2	Durante el empleo.				
	8.2.1	Responsabilidades de la Dirección.		X		
	8.2.2	Concienciación, formación y capacitación en seguridad de la información.			X	
	8.2.3	Proceso disciplinario.	X			
	8.3	Finalización o cambio del empleo.				
	8.3.1	Responsabilidad del cese o cambio.		X		
	8.3.2	Devolución de activos.		X		
	8.3.3	Retirada de los derechos de acceso.		X		

Fuente: Elaboración propia

E. Seguridad física y del entorno

a. Hallazgos:

El Jefe de Tecnología de la Información, administra los sistemas de información del CGT, no cuenta con políticas o parámetros de seguridad para poder garantizar la confidencialidad de la información que maneja, no se les restringe el pase a ninguna persona y tampoco se lleva el control de acceso a esta área por parte del personal encargado.

No se designa y aplica adecuadamente una protección física contra amenazas externas y ambientales tales como del fuego, inundación, terremoto o alguna otra forma de desastre natural o humano.

El CGT si cuenta con un Sistema de Alimentación Ininterrumpida (UPS) para el funcionamiento continuo de los equipos que soporten operaciones críticas de la organización.

En la red de cableado, utilizan cable de categoría 5, así mismo existen serios daños en este aspecto. Se mostrara una lista con los daños encontrados en las diferentes áreas del CGT.

Situación Actual de red de cableado:

- En algunas áreas el cielo raso estaba en mal estado.
- El cable de red en algunas zonas estaba deteriorado
- Cable de red dificultado el paso de las personas.
- El cableado de la red se encuentra junto al de la red eléctrica.
- No se restringe el acceso a personas no autorizadas a los dispositivos de red (Routers y Switches).
- Varios conectores de pared no se encuentran fijos.
- Cableado sin identificadores.
- Cableado suelto.
- Cableado con distancias que sobrepasa la norma
- Cableado sin protección (no están debidamente canaleteados).

Por estos daños encontrados coexisten una serie de problemas para todos los usuarios de TI del CGT en el desempeño adecuado de sus labores ya que en muchas ocasiones pierden la conexión a internet o a los sistemas. Así mismo lo equipos de TI del CGT se mantienen adecuadamente ya que el personal de mantenimiento de la Oficina de TI se encargan de realizar la reparación y servicio de los equipos. Además registran documentalmente todos los fallos encontrados, como se observa en el documento de Bitácora de Soporte Técnico Presencial, sin embargo este proceso de soporte técnico no se encuentra debidamente documentado.

b. Consecuencias:

La Oficina de TI al no contar con controles físicos de entrada pone en riesgo sus equipos de trabajo, así mismo deja vulnerable las bases de datos del sistema, pudiendo ser esto perjudicial para la información que posee. Esta situación se presta para robos y daños de equipos. Al no contar con controles ante amenazas externas y ambientales podría verse afectado la disponibilidad e integridad de los activos de información del CGT.

En cuanto a los problemas detectados en la red de cableado podría generarse interrupción en el acceso a internet o algún otro sistema y por consiguiente se vería afectado algunas actividades que desempeña el personal del CGT.

c. Cumplimiento del SOA

Tabla N° 16. Cumplimiento del dominio de Seguridad Física y del Entorno

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Seguridad Física y del Entorno	9.1	Áreas seguras.				
	9.1.1	Perímetro de seguridad física.		X		
	9.1.2	Controles físicos de entrada.			X	
	9.1.3	Seguridad de oficinas, despachos e instalaciones.			X	
	9.1.4	Protección contra las amenazas externas y de origen ambiental.			X	
	9.1.5	Trabajo en áreas seguras.		X		
	9.1.6	Áreas de acceso público y de carga y descarga.				X
	9.2	Seguridad de los equipos.				
	9.2.1	Emplazamiento y protección de equipos.		X		
	9.2.2	Instalaciones de suministro.		X		
	9.2.3	Seguridad del cableado.			X	
	9.2.4	Mantenimiento de los equipos.		X		
	9.2.5	Seguridad de los equipos fuera de las instalaciones.			X	
	9.2.6	Reutilización o retirada segura de equipos.			X	
	9.2.7	Retirada de materiales propiedad de la empresa.			X	

Fuente: Elaboración propia

F. Gestión de Comunicaciones y Operaciones.

a. Hallazgos:

No se controla los cambios en los sistemas y recursos de tratamiento de información, como tampoco se identifican y registran los cambios significativos, ni se evalúan los posibles impactos de dichos cambios.

No existen políticas definidas para la elaboración de manuales de sus procesos informáticos, ningún proceso que realiza el área de Gerencia de Tecnología de la Información se encuentra documentado ya que no se cuenta con la obligatoriedad para la elaboración de dichos manuales de sus procesos que realiza.

Entre los procesos informáticos que realiza la Oficina de TI tenemos:

- Backup: Se realiza una copia de Seguridad a la base de Datos de los sistemas y aplicaciones.
- Soporte Técnico.
- Administrar las redes y comunicaciones

Por otra parte no existen políticas de segregación de funciones, el CGT no cuenta con la implementación de la segregación de tareas en todos sus aplicativos.

En el CGT es poco común la realización de un pase de versión de un aplicativo. Así mismo, la Oficina de TI no cuentan con un proceso de desarrollo de software ya que los sistemas que utilizan, han sido desarrollados por terceros, pero algunos sistemas que necesitan lo dejan de tarea a los desarrolladores, quienes son ellos que elaboran sistemas hechos a medida sin embargo en el desarrollo de estos sistemas no se identifican ni implementan controles adecuados para el nivel de separación entre los entornos de desarrollo, prueba y producción que es necesario para evitar problemas operacionales.

No se cuenta con un procedimiento para la atención de errores, en caso se encuentre un error en alguna aplicación el personal de sistemas trata de corregirlo por experiencia propia.

El personal de la Oficina de TI mantiene un monitoreo constante del rendimiento de los servidores y servicios del CGT.

En el caso de protección de código malicioso, hacen uso de antivirus; sin embargo no cuentan con una política de antivirus,

así mismo no controlan el licenciamiento de este, ya que actualmente se encuentra desactualizado.

No se cuenta con un procedimiento de backups el cual detalle el esquema de respaldos que utiliza el personal de sistemas, esto lo realiza una persona de la Oficina de TI por experiencia propia.

En base a los errores de aplicativos, estos son verificados cuando surge una falla en alguno de ellos, sin embargo no existe un procedimiento frecuente de los mismos.

b. Consecuencias:

Al no contar con un control que permita manejar los cambios en las operaciones, el riesgo es que no se realicen los controles necesarios para la gestión oportuna de los cambios en la organización, los procesos del negocio, las instalaciones de procesamiento de la información, y sistemas que puedan afectar la seguridad de la información, generando fallas y vulnerabilidades al sistema.

Al no implantar la segregación de tareas en seguridad de la información, se podría aumentar el riesgo de un mal uso del sistema deliberado o por negligencia.

Al no identificar e implementar controles adecuados para el nivel de separación entre los entornos de desarrollo, prueba y producción se generaría problemas operacionales. Las actividades de desarrollo y prueba pueden causar serios problemas, por ejemplo, cambios no deseados en los archivos o en el entorno del sistema o fallos del sistema. Así mismo si el personal de desarrollo y el de prueba tuvieran acceso al sistema de producción y a su información, podrían introducir un código no autorizado o no probado o alterar los datos operacionales.

Al no concientizar a los usuarios sobre seguridad de la información estos podrían introducir software malicioso a sus equipos informáticos con los que laboran.

Al no contarse con un procedimiento de Backup no se podría en algún momento recuperar cierta información tras un desastre o un fallo de los medios, así mismo si renunciara la única persona que realiza este procedimiento por experiencia propia, el personal que lo suplante no sabría qué aspectos tener en cuenta para este proceso.

c. Cumplimiento del SOA:

Tabla N° 17. Cumplimiento del dominio de Seguridad de las Comunicaciones y Operaciones

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
	10.1	Responsabilidades y procedimientos de operación.				
	10.1.1	Documentación de los procedimientos de operación.			X	
	10.1.2	Gestión de cambios.			X	
	10.1.3	Segregación de tareas.			X	
	10.1.4	Separación de los recursos de desarrollo, prueba y operación.			X	
	10.2	Gestión de la provisión de servicios.				
	10.2.1	Provisión de servicios.			X	
	10.2.2	Supervisión y revisión de los servicios prestados por terceros.			X	
	10.2.3	Gestión del cambio en los servicios prestados por terceros.			X	
	10.3	Planificación y aceptación del sistema.				
	10.3.1	Gestión de capacidades.			X	
	10.3.2	Aceptación del sistema.			X	
	10.4	Protección contra el código malicioso y descargable.				
	10.4.1	Controles contra el código malicioso.		X		
	10.4.2	Controles contra el código descargado en el cliente.		X		
	10.5	Copias de seguridad.				
	10.5.1	Copias de seguridad de la información.		X		
	10.6	Gestión de seguridad en redes.				
	10.6.1	Controles de red.		X		
	10.6.2	Seguridad de los servicios de red.		X		
Gestión de Comunicaciones y operaciones	10.7	Manipulación de los soportes.				
	10.7.1	Gestión de soportes extraíbles.			X	
	10.7.2	Retirada de soportes.		X		
	10.7.3	Procedimientos de manipulación de la información.			X	
	10.7.4	Seguridad de la documentación del sistema.		X		
	10.8	Intercambio de información.				
	10.8.1	Políticas y procedimientos de intercambio de información.			X	
	10.8.2	Acuerdos de intercambio.			X	
	10.8.3	Soportes físicos en tránsito.			X	
	10.8.4	Mensajería electrónica.			X	

	10.8.5	Sistemas de información empresariales.		X		
	10.9	Servicios de comercio electrónico.				
	10.9.1	Comercio electrónico.				X
	10.9.2	Transacciones en línea.				X
	10.9.3	Información públicamente disponible.		X		
	10.10	Supervisión.				
	10.10.1	Registros de auditoría.			X	
	10.10.2	Supervisión del uso del sistema.			X	
	10.10.3	Protección de la información de los registros.			X	
	10.10.4	Registros de administración y operación.			X	
	10.10.5	Registro de fallos.		X		
	10.10.6	Sincronización del reloj.			X	

Fuente: Elaboración propia

G. Control de Accesos

a. Hallazgos:

La base de datos de los sistemas que maneja la Oficina de TI de las aplicaciones que utiliza el CGT, no cuenta con controles de accesos físicos (para proteger a los equipos de amenazas externas) ni lógicos (aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo). Es muy fácil acceder al sistema y verificar sus datos, pues, solamente está protegidos los equipos con contraseña de apertura al mismo pero una vez habiendo ingresado, se puede explorar el entorno y manipular la información del sistema y su base de datos puesto que no cuenta con seguridad de acceso al sistema. No cuenta con módulos de seguridad para acceder a los datos. No cuenta con mecanismos de acceso como: Identificación, autenticación y autorización.

El CGT no cuenta con perfiles de usuarios, tan solo se tiene ciertos roles para los accesos.

El responsable de control de accesos retira los accesos cuando se entera por casualidad de la desvinculación de un empleado, en pocos casos la Unidad de Recursos Humanos le notifica la salida del personal.

Actualmente el CGT no ha realizado concientización de los empleados sobre las responsabilidades o condiciones al otorgarle accesos a la red y aplicativos en general.

No existe una política que exija que cada vez que se le otorgue una contraseña a un usuario para acceso a cualquier recurso, esta debe nacer expirada, solo se tiene como buena práctica de seguridad, pero esta no está ni documentada.

Para el acceso a un determinado sistema el personal solicitante envía un documento a la Gerencia de Tecnología de la Información, con un requerimiento pidiendo la instalación de dicho sistema y el motivo de por qué lo solicita.

Además no se tiene un sistema para la administración de accesos a los diferentes aplicativos. También no se cuenta con un procedimiento para la notificación del estado de los usuarios de TI del CGT entiéndase por: cambio de área, vacaciones, licencia por maternidad o enfermedad.

No se tiene normas sobre la confidencialidad de sus claves de acceso. No se ha realizado campañas de concientización sobre seguridad de la información.

El responsable de autorizar el acceso a la red y al servicio de red es del jefe de la Gerencia de Tecnología de la Información.

No cuentan con una política de escritorio limpio que especifique que no se pueda instalar programas no autorizados en los equipos de cómputo, es por ello que cualquier usuario instala diversos programas a su equipo sin consultarle al Oficina de TI previamente.

b. Consecuencias:

Al contar con un uso inapropiado de los privilegios de la administración del sistema pueden ser un gran factor contribuidor de fallas o aberturas en los sistemas.

Al no otorgarles responsabilidades a los usuarios de TI del CGT, se generaría el acceso de usuarios no autorizados e incluso el hurto de la información y de las instalaciones del procesamiento de información.

Al no contar con una política de escritorio limpio se incrementaría el riesgo de acceso no autorizado o de daño a los medios e instalaciones del procesamiento de información.

Al no prevenir adecuadamente mediante políticas el acceso no autorizado a los aplicativos del CGT, se podría comprometer la seguridad de dichos sistemas.

c. Cumplimiento del SOA:

Tabla N° 18. Cumplimiento del dominio de Control de Accesos

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Control de Acceso	11.1	Requisitos de negocio para el control de acceso.				
	11.1.1	Política de control de acceso.			X	
	11.2	Gestión de acceso de usuario.				
	11.2.1	Registro de usuario.		X		
	11.2.2	Gestión de privilegios.		X		
	11.2.3	Gestión de contraseñas de usuario.		X		

	11.2.4	Revisión de los derechos de acceso de usuario.		X		
	11.3	Responsabilidades de los usuarios.				
	11.3.1	Uso de contraseñas.		X		
	11.3.2	Equipo de usuario desatendido.		X		
	11.3.3	Política de puesto de trabajo despejado y pantalla limpia.			X	
	11.4	Control de acceso a la red.				
	11.4.1	Política de uso de los servicios en red.			X	
	11.4.2	Autenticación de usuario para conexiones externas.			X	
	11.4.3	Identificación de los equipos en las redes.		X		
	11.4.4	Protección de los puertos de diagnóstico y configuración remotos.		X		
	11.4.5	Segregación de las redes.			X	
	11.4.6	Control de la conexión a la red.		X		
	11.4.7	Control de encaminamiento (routing) de red.			X	
	11.5	Control de acceso al sistema operativo.				
	11.5.1	Procedimientos seguros de inicio de sesión.			X	
	11.5.2	Identificación y autenticación de usuario.		X		
	11.5.3	Sistema de gestión de contraseñas.		X		
	11.5.4	Uso de los recursos del sistema.		X		
	11.5.5	Desconexión automática de sesión.			X	
	11.5.6	Limitación del tiempo de conexión.			X	
	11.6	Control de acceso a las aplicaciones y a la información.				
	11.6.1	Restricción del acceso a la información.		X		
	11.6.2	Aislamiento de sistemas sensibles.		X		
	11.7	Ordenadores portátiles y teletrabajo.				
	11.7.1	Ordenadores portátiles y comunicaciones móviles.				X
	11.7.2	Teletrabajo.				X

Fuente: Elaboración propia

H. Adquisición, desarrollo y mantenimiento de sistemas de información

a. Hallazgos:

En cuanto a la adquisición de algún software por parte del CGT solo se utilizan las buenas prácticas de seguridad ya que no existen políticas de la adquisición o desarrollo del software.

La Oficina de TI no desarrollan aplicaciones, pero si por algún motivo tengan que desarrollar alguna, esta labor lo realizan en algunos casos los practicantes que laboran en el área.

Se puede producir una fuga de información, ya que no se cuenta con controles para la protección de la información, en estos casos es fácil extraerse la información del CGT sin que existan alertas de acceso no autorizados.

Actualmente la gran mayoría de usuarios de TI no tiene deshabilitado los puertos USB y es por esta vía se puede extraer información valiosa del CGT.

b. Consecuencias:

Al no contar con un procedimiento para el desarrollo y mantenimiento de Software, el riesgo es que no se cumpla las disposiciones y prácticas definidas, lo que puede incidir en el diseño e implementación de los requisitos de seguridad de la información durante el ciclo de vida de desarrollo, lo que puede generar vulnerabilidades en los sistemas del CGT.

Al no darle la seguridad adecuada a las aplicaciones del sistema, estas podrían sufrir alguna modificación o mal uso de los datos de usuario. Así mismo los datos ingresados podrían ser corrompidos por errores de hardware, procesamiento de errores o a través de actos deliberados.

Al no asegurarse la revisión de todo cambio propuesto al sistema se podría debilitar la seguridad al sistema o sistema operativo.

Al no tener un control de las actualizaciones automáticas de los sistemas, podría causar que alguna actualización genere fallos en el sistema o sistema operativo.

c. Cumplimiento del SOA:

Tabla N° 19. Cumplimiento del dominio de adquisición, desarrollo y mantenimiento de sistemas de información

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Adquisición, desarrollo y mantenimiento de Sistemas de Información	12.1	Requisitos de seguridad de los sistemas de información.				
	12.1.1	Análisis y especificación de los requisitos de seguridad.			X	
	12.2	Tratamiento correcto de las aplicaciones.				
	12.2.1	Validación de los datos de entrada.		X		
	12.2.2	Control del procesamiento interno.		X		
	12.2.3	Integridad de los mensajes.			X	
	12.2.4	Validación de los datos de salida.		X		
	12.3	Controles criptográficos.				
	12.3.1	Política de uso de los controles criptográficos.				X
	12.3.2	Gestión de claves.				X
	12.4	Seguridad de los archivos de sistema.				
	12.4.1	Control del software en producción.		X		
	12.4.2	Protección de los datos de prueba del sistema.		X		
	12.4.3	Control de acceso al código fuente de los programas.		X		

	12.5	Seguridad en los procesos de desarrollo y soporte.				
	12.5.1	Procedimientos de control de cambios.			X	
	12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.		X		
	12.5.3	Restricciones a los cambios en los paquetes de software.		X		
	12.5.4	Fugas de información.			X	
	12.5.5	Externalización del desarrollo de software.				X
	12.6	Gestión de la vulnerabilidad técnica.				
	12.6.1	Control de las vulnerabilidades técnicas		X		

Fuente: Elaboración propia

I. Gestión de Incidentes en la seguridad

a. Hallazgos:

No se cuenta con políticas y procedimientos de gestión y reporte de incidencias, sin embargo si se cuenta con un formato de Reporte de Incidencia Informática y un formato de Registro de reportes de Incidencias Informáticas, esto significa que la Oficina de TI si contiene evidencias de los incidentes de seguridad, aunque estos no están debidamente procedimentados.

Así mismo también se evidencio un Acta de Traslado de Equipo, para aquellos equipos que tienen alguna incidencia y colocan la forma como solucionar esa avería en el Acta de Medida Correctora Aplicada.

Falta realizar procesos de concientización sobre seguridad de la información es por ello que no saben a quién notificar de alguna incidencia detectada.

Actualmente el personal del CGT no tiene conocimiento de cómo actuar ante un incidente de seguridad, así mismo no se tienen definidas las responsabilidades ante un evento de seguridad.

b. Consecuencias:

El CGT al no contar con políticas de gestión de incidentes no podrá dar tratamiento oportuno y adecuado a los incidentes de seguridad de la información, además de hacerse cargo de las pérdidas derivadas. Sin estos procedimientos no podrán revertir las situaciones y mitigar los efectos de los incidentes de seguridad de la información.

Como no se tiene un conocimiento por parte de todo el personal del CGT en reportar eventos y debilidades de la seguridad de información, estos incidentes no se reportan a tiempo por lo tanto no se solucionan lo más rápido posible.

c. Cumplimiento del SOA:

Tabla N° 20. Cumplimiento del dominio de gestión de incidentes de la seguridad de la información

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Gestión de incidentes de la seguridad de la Información	13.1	Reportando eventos y debilidades de la seguridad de la información.				
	13.1.1	Notificación de los eventos de seguridad de la información.		X		
	13.1.2	Notificación de puntos débiles de seguridad.		X		
	13.2	Gestión de incidentes y mejoras de seguridad de la información.				
	13.2.1	Responsabilidades y procedimientos.			X	
	13.2.2	Aprendizaje de los incidentes de seguridad de la información.			X	
	13.2.3	Recopilación de evidencias.		X		

Fuente: Elaboración propia

J. Gestión de la continuidad del negocio

a. Hallazgos:

No se cuenta con un plan de gestión para el desarrollo y el mantenimiento de la continuidad del negocio en el cual el CGT trate los requerimientos en la seguridad de la información necesarios para la continuidad del negocio. Así también los eventos que pueden causar interrupciones a los procesos de negocio del CGT no están debidamente identificados

b. Consecuencias:

Al no contar con un plan de continuidad del Negocio, podría darse el caso que ante la ocurrencia de una situación de catástrofe o interrupción de las actividades, no se puedan recuperar las actividades de manera oportuna. Así mismo al no contar con este plan generaría una falta de garantía a que los procesos y actividades internas no se realicen de una forma adecuada a las necesidades del CGT, como también aumentaría el riesgo de incidentes de seguridad de la información y la dificultad en garantizar la confidencialidad, integridad y disponibilidad de las informaciones.

Sin un plan de continuidad del negocio no se analizaría las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio, por consiguiente no

se desarrollaría e implantaría planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos.

c. Cumplimiento del SOA:

Tabla N° 21. Cumplimiento del dominio de gestión de la continuidad del negocio

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Gestión de la continuidad del negocio	14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.				
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.			X	
	14.1.2	Continuidad del negocio y evaluación de riesgos.			X	
	14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.			X	
	14.1.4	Marco de referencia para la planificación de la continuidad del negocio.			X	
	14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.			X	

Fuente: Elaboración propia

K. Cumplimiento

a. Hallazgos:

No existen procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el uso de productos de software propietario del CGT. El Gerente de TI del CGT no se asegura que se cumpla correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad cumpliendo las políticas y estándares de seguridad que existen.

b. Consecuencias:

Al no contar con una política de cumplimiento con los requisitos legales originaria que no se protejan los registros importantes de la organización y estos registros estén vulnerables a pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio. Al no realizarse

auditorias de seguridad de información no se realizarían revisiones de la políticas de seguridad, así como no se verificarían que tan efectivos son los controles que se han implementado.

c. Cumplimiento del SOA:

Tabla N° 22. Cumplimiento del dominio de Cumplimiento

CONTROLES ISO 27002:2005			Efectividad del Control			
Clausula	**SEC**	**Control/Objetivo de Control**	**Cumple**	**Cumple Parcial**	**No Cumple**	**No Aplica**
Cumplimiento	15.1	Cumplimiento con los requisitos legales.				
	15.1.1	Identificación de la legislación aplicable.		X		
	15.1.2	Derechos de propiedad intelectual (DPI).		X		
	15.1.3	Protección de los documentos de la organización.		X		
	15.1.4	Protección de datos y privacidad de la información de carácter personal.		X		
	15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.		X		
	15.1.6	Regulación de los controles criptográficos.				X
	15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.				
	15.2.1	Cumplimiento de las políticas y normas de seguridad.			X	
	15.2.2	Comprobación del cumplimiento técnico.			X	
	15.3	Consideraciones sobre las auditorías de los sistemas de información.				
	15.3.1	Controles de auditoría de los sistemas de información.			X	
	15.3.2	Protección de las herramientas de auditoría de los sistemas de información.			X	

Fuente: Elaboración propia

1.4. Evaluación de la seguridad de la Información del CGT

Para la presente evaluación se utilizó como base la norma NTP ISO/IEC 27002:2005, bajo el modelo de madurez CMM, para poder mostrar su nivel de cumplimiento en el CGT y con ello, poder ver reflejado el nivel de implementación de los diferentes dominios de la norma.

La evaluación se hace sobre los 11 dominios de la norma NTP ISO/IEC 27002:2005, evaluado bajo el modelo de madurez de capacidad CMM a los 133 controles de la presente norma.

Así mismo para hacer esta evaluación de la seguridad de la información del CGT, se realizó un cuestionario, en el cual se tomó cada uno de los controles de esta norma y se calificaron acorde a la siguiente tabla:

Tabla N° 23. Clasificación del Modelo de Madurez CMM

Nivel	CMM	Efectividad	Descripción
Inexistente	L0	0%	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
Inicial / Ad-hoc	L1	10%	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
Reproducible, pero intuitivo	L2	50%	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
Proceso definido	L3	90%	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
Gestionado y medible	L4	95%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
Optimizado	L5	100%	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.
No Aplica	N/A	N/A	El control no es aplicable a la organización.

Fuente: Elaboración Propia

a. Nivel de implantación basado en CMM

La siguiente tabla muestra el nivel de implementación de los controles, según el resultado del cuestionario realizado:

Tabla N° 24. Resultado de Calificación CMM

NTP ISO/IEC 27002			
#	Dominio	Estado actual	Estado deseado
5	Política de seguridad	10%	60%
6	Aspectos Organizativos de la seguridad de la información.	20%	60%
7	Clasificación y Control de activos.	41%	60%
8	Seguridad en recursos humanos	59%	60%
9	Seguridad física y del entorno	27%	60%
10	Gestión de comunicaciones y operaciones.	25%	60%
11	Control de acceso.	34%	60%
12	Adquisición, desarrollo y mantenimiento de Sistemas de Información	37%	60%
13	Gestión de incidentes	35%	60%
14	Gestión de continuidad de negocio	10%	60%
15	Cumplimiento	30%	60%

Fuente: Elaboración propia adaptado del Resultado del Cuestionario NTP ISO/IEC 27002:2005

Podemos observar que la mayoría de los dominios están por debajo del 40%, e incluso hay muy bajos resultados en 2 dominios, las políticas de seguridad con un 10%, y Gestión de continuidad de negocio con un 10% los cuales se necesitan mejorar.

También se puede observar que existen 2 buenos resultados en los dominios de clasificación y control de activos con un 41% y seguridad en recursos humanos con un 59%. Sin embargo, el resultado general es de un 30% lo que significa que se deben mejorar algunos controles para poder llegar al estado deseado del 60% (estado que se asemeja a la realidad situacional del CGT)

b. Resultados según CMM

A continuación se entrega el nivel de cumplimiento, nivel de madurez CMM de la norma NTP ISO/IEC 27002:2005:

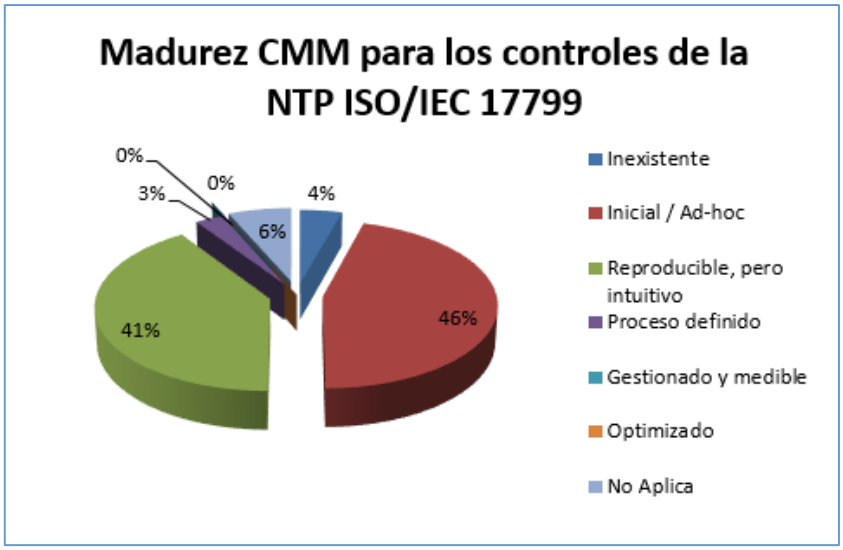


Figura N° 15. Madurez CMM para los controles de la NTP ISO/IEC 27002
Fuente: Elaboración propia adaptado del Resultado del Cuestionario NTP ISO/IEC 27002:2005

Vemos como, el mayor porcentaje está entre los controles que poseen un proceso inicial/Ad-hoc y los que son reproducibles, pero intuitivos. Es importante resaltar que existe un porcentaje de 4% de controles "inexistentes", y que además no hay porcentaje para controles Gestionados y medibles, ni controles optimizados eso indica que es necesario implementar un modelo de un Sistema de Gestión de Seguridad de Información que ayude a mejorar los controles existentes e implementar nuevos para mejorar los procesos de TI en el CGT.

c. Conclusiones de la evaluación de madurez.

El nivel de cumplimiento del CGT frente a los requerimientos de la norma NTP ISO/IEC 27002:2005, es del 30%, lo que significa que la implementación del Sistema de Gestión de Seguridad de la información le implicará a la institución un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos. Sin embargo con el modelo del SGSI planteado se lograría implementar nuevos controles, mejorar los controles existentes para así poder acercarse al estado deseado.

II. MARCO TEÓRICO

2.1. Antecedentes de otras investigaciones

De la revisión literaria, se describe a continuación los antecedentes a la investigación que se tomarán en cuenta en el diseño del Sistema de Gestión de la Seguridad de la Información propuesto.

TITULO	Evaluación técnica de seguridades del data center del municipio de Quito según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005
UNIVERSIDAD	Universidad de las fuerzas armadas ESPE, Sede SANGOLQUI (Ecuador)
FECHA	2014
AUTOR(ES)	Ing. Diego Santiago Aguirre Freire Ing. Jhon Carlos Palacios Cruz
RESUMEN	Este presente estudio es aplicado al municipio de Quito la cual maneja información sensible de la ciudadanía y esta se encuentra alojada en los servidores y sistemas de almacenamiento ubicados en el Data center, por lo que para garantizar su confidencialidad, integridad y disponibilidad se hizo una evaluación técnica informática para determinar el cumplimiento de las normas y estándares que se deben seguir para una adecuada gestión de seguridad de la información, utilizando para ello las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005. Según esta evaluación técnica se pudo identificar las vulnerabilidades de seguridad en todos los elementos que se encuentran en Data Center y con ello se pudo recomendar políticas de seguridad de la información y la implementación de controles para el manejo de riesgos, monitoreo y revisión del desempeño y efectividad del Data Center, considerando el mejoramiento continuo de la seguridad.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	La relación está en que la evaluación técnica de seguridad realizada en esta investigación utiliza como marco de referencia la ISO/IEC 27001, la cual será parte de nuestro estudio, así mismo tendremos como referencia los correctivos aplicados, las políticas, procesos y controles de seguridad propuestos. Además como este estudio se realizó en un municipio se puede tomar la metodología utilizada y orientarla al desarrollo de nuestra investigación.

TITULO	DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. CASO: DIRECCIÓN DE INFORMÁTICA DE LA ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA.
UNIVERSIDAD	Universidad Centoccidental "Lisandro Alvarado", Sede Venezuela
FECHA	2011
AUTOR(ES)	Ing. Arelys Altagracia López M.
RESUMEN	La presente investigación tiene como objetivo fundamental diseñar un Plan de Gestión de Seguridad de la Información en la Alcaldía del Municipio Jiménez del Estado Lara, el cual le permitió a la institución determinar los objetivos, procesos y procedimientos para el establecimiento de políticas de seguridad, así como de un conjunto de controles de seguridad que ayudarán a gestionar los riesgos en la Seguridad de la Información que maneja el organismo objeto de estudio, mejorando de esta forma la gestión de los incidentes de seguridad que se detecten y generando resultados en concordancia con los objetivos y políticas requeridas todo ello dentro del marco de la norma ISO/IEC 27000.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Este estudio permite orientar el desarrollo de esta investigación para el CGT, porque el diseño del plan de gestión de seguridad de la información propuesto está basado en la norma ISO 27001, que es el estándar que tomaremos de referencia en este trabajo.

TITULO	IMPLEMENTACIÓN DE LOS CONTROLES ASIGNADOS AL DOMINIO "GESTIÓN DE ACTIVOS", BAJO LOS LINEAMIENTOS ESTABLECIDOS POR LA NORMA ISO/27001 ANEXO A, PARA LAS EMPRESAS MUNICIPALES DE CALI, EMCALI E.I.C.E-ESP.
UNIVERSIDAD	Universidad Autónoma de Occidente, sede Colombia
FECHA	2013
AUTOR(ES)	PAUL ROSEMBERG ENRIQUEZ ESPINOSA
RESUMEN	Este estudio busca implementar el dominio de GESTION DE ACTIVOS el cual se encuentra incluido dentro del anexo A de la Norma ISO 27001, con el fin de que los controles concernientes a este dominio sean encaminados a garantizar la confidencialidad, integridad,

	disponibilidad y trazabilidad de los activos de información que posee la Gerencia Tecnología de la Información y sus departamentos asociados, contribuyendo de esta manera a la correcta implementación del Sistema de Gestión de Seguridad de la Información para las empresas municipales de CALI(EMCALI).
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	La tesis tiene relación con esta propuesta ya que la solución planteada tiene que ver con la implementación de controles que están bajo los lineamientos establecidos por la norma ISO/IEC 27001, permitiendo minimizar el riesgo sobre los activos de información, mediante la identificación de activos críticos, políticas para el buen uso de los activos de información y la generación de cultura y hábitos de seguridad respecto a la seguridad de la información en los empleados de la organización, garantizando de esta manera la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información. Es por ello que podemos evaluar el proceso que siguió durante la implementación de estos controles y de esa forma poder orientar el desarrollo de este estudio para el Centro de Gestión Tributaria de Chiclayo.

TITULO	DISEÑO DE PROCEDIMIENTOS DE AUDITORÍA DE CUMPLIMIENTO DE LA NORMA NTP-ISO/IEC 17799:2007 COMO PARTE DEL PROCESO DE IMPLANTACIÓN DE LA NORMA TÉCNICA NTP-ISO/IEC 27001:2008 EN INSTITUCIONES DEL ESTADO PERUANO
UNIVERSIDAD	Pontificia Universidad Católica del Perú - Lima-Perú
FECHA	2014
AUTOR(ES)	Huamán Monzón, Fernando Miguel
RESUMEN	El presente proyecto responde a la necesidad creada a causa de las normativas publicadas por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) que declaran de uso obligatorio las Normas Técnicas Peruanas NTP-ISO/IEC 27001:2008 y NTP-ISO/IEC 17799:2007 a una lista de empresas del estado peruano que pertenezcan y/o estén involucradas en la Administración Pública con la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información de la misma. Así mismo esta investigación tiene como objetivo establecer un procedimiento de auditoría de cumplimiento para la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 en las

	instituciones del Estado Peruano basado en el marco COBIT 5.0, como parte del proceso de implantación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 con la finalidad de mejorar la gestión de la seguridad de la información.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	La relación con la investigación está dada por la aplicación de las normas peruanas NTP ISO/IEC 27001 y NTP ISO/IEC 17799 las cuales son importantes para que las empresas de gobierno peruano implementen un plan de seguridad de la información y así poder establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración pública.

TITULO	Diseño De Un Sistema De Gestión De Seguridad De La Información Para Una Entidad Estatal De Salud De Acuerdo A La ISO/IEC 27001:2013
UNIVERSIDAD	Pontificia Universidad Católica del Perú- Lima-Perú
FECHA	2015
AUTOR(ES)	Vasco Rodrigo Talavera Álvarez
RESUMEN	La presente investigación busca desarrollar el Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud – el Instituto Nacional Materno Perinatal – sujeta al cumplimiento de la normativa vigente relativa a Seguridad de la Información, la Norma Técnica NTP ISO/IEC 27001 con la finalidad de asegurar el buen uso y protección de la información crítica que manejan, ya sea de clientes o información estratégica interna.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	La relación con la investigación está dada por la aplicación de la Norma Técnica Peruana NTP ISO/IEC 27001, la cual exige que las entidades públicas realicen la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo las recomendaciones y controles señalados en la misma.

2.2. Base teórica

Para el desarrollo del presente proyecto de tesis, es necesario tener en cuenta los siguientes fundamentos teóricos:

2.2.1. Sistema de Gestión de Seguridad de la información

A. Información

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada (NTP ISO/IEC 17799, 2007).

Por su parte, los autores Andreu, Ricart y Valor (1998) explican como la información se convierte en un recurso estratégico para las empresas y se integra dentro de su proceso de planificación estratégica.

Así entonces la información se ha convertido en un recurso clave para las empresas a todos los niveles jerárquicos y para todos los departamentos ya que las organizaciones deben conseguir, procesar, usar y comunicar información, tanto interna como externa, en sus procesos de planificación, dirección y toma de decisiones. (Carrasco, 2010)

Por lo tanto este recurso el cual puede adoptar diferente formas ya sea impresa o escrita en papel, trasmitida por algún medio electrónico, mostrada en video o simplemente hablada en conversación sigue siendo importante para una empresa ya que para la labor de un directorio o algún otro responsable la información tiene la función clave de minimizar la incertidumbre en la toma de decisiones así que esta debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

B. Activo de información

Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Estos son necesarios para que la organización funcione y alcance los objetivos que propone su dirección. (Espinoza, 2013)

Según el contexto de la ISO/IEC 17799 (2005), Código de Práctica para la Gestión de Seguridad de Información, un activo de información es: “Algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger”.

La NTP-ISO/IEC 27005 (2009) clasifica el activo en dos tipos:

- Los activos primarios: Son usualmente los procesos e información centrales de la actividad en cuestión. Otros activos primarios como los procesos de la organización también pueden considerarse, lo cual será más apropiado para diseñar una política de seguridad de la información o un plan de continuidad del negocio.
    - Procesos y actividades de negocio
    - Información
- Los activos de apoyo: Estos activos tienen vulnerabilidades que son explotables por amenazas que tienen como objetivo desactivar los activos primarios del alcance (proceso e información). Son de varios tipos:
    - Hardware
    - Software
    - Red
    - Personal
    - Sitio
    - Estructura de la Organización

C. Propietario del activo de información

Según la NTP-ISO/IEC 27005 (2009), el propietario del activo es aquel que puede no tener derechos de propiedad sobre el activo, pero tiene responsabilidad sobre su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo a menudo es la persona más apropiada para determinar el valor que el activo tiene para la organización. Se debe identificar al propietario de un activo para cada activo, para determinar las disposiciones sobre responsabilidad y rendición de cuentas por el activo.

D. Seguridad

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros. (Villalón Huerta, 2002)

Por lo tanto la seguridad se relaciona a la manera como se puede eliminar la incertidumbre ante lo que puede ocurrir, teniendo siempre en cuenta que la seguridad al 100% no existe, así mismo Corletti (2007) explica que mediante normas o una serie de medidas se puede buscar una mejora continua, esto aumentara el porcentaje actual de seguridad en cualquier empresa. Esta mejora en la seguridad se ve reflejada en una serie de ventajas haciéndola a la empresa más competitiva.

E. Seguridad de la Información

Sabiendo que la información de toda empresa es un activo importante, y que se encuentra expuesta a un gran número de amenazas internas como externas, cuyo origen puede ser natural o consecuencia del hombre, ya sea de forma deliberada o accidental, es necesario que se establezcan medidas para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas asegurando apropiadamente su resguardo.

La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios. (NTP ISO/IEC 17799, 2007)

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad de la organización. (NTP ISO/IEC 17799, 2007)

La seguridad de información es importante en negocios tanto del sector público como del privado y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, por ejemplo lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. (NTP ISO/IEC 17799, 2007)

Así mismo la ISO/IEC 27001 (2005) define Seguridad de la Información (SI) como: La preservación de la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización. Además, también pueden estar involucradas otras propiedades como son: la autenticidad, la responsabilidad, el no-repudio y la confiabilidad.

También es muy importante tener en claro que la seguridad de tecnologías de información y la seguridad de información son conceptos diferentes: la seguridad de TI se encarga en particular, de la protección tecnológica y es gestionada desde un nivel operativo por las áreas de sistemas de las organizaciones.

La seguridad de información va más allá ocupándose de riesgos, beneficios, buen uso, procesos y actividades involucradas con la información y los activos relacionados a ella, impulsados por la Alta Dirección empresarial. (Tupia Anticona, 2011)

Principios de la seguridad de la Información

Los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se provocan daños irreparables. (Montesino, Baluja y Porven, 2013)

Estos últimos tres términos constituyen la base de la seguridad de la información, de donde se resume la explicación que se da a continuación.

a. **Confidencialidad**

Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. La información, dentro y fuera de una organización, no siempre puede ser conocida por cualquier individuo, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos. La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, como durante su procesamiento y tránsito, hasta llegar a su destino final. (Condori Alejo, 2012)

b. **Integridad**

Este principio permite garantizar que la información no sea modificada o alterada en su contenido por personas no autorizados o de forma indebida. Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos.

c. Disponibilidad

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Adicionalmente, la disponibilidad hace referencia a la capacidad que deben tener los sistemas de recuperarse ante interrupciones del servicio, de una manera segura que garantice el continuo desarrollo de la productividad de la organización sin mayores inconvenientes. (Condori Alejo, 2012)

F. Políticas de Seguridad de la Información

Una política de seguridad de la información es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. (Hernández Pinto, 2006)

Tiene como objetivo de dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones. La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización. (NTP ISO/IEC 17799, 2007)

Peltier, considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo. (Peltier, Peltier, & Blackley, 2005)

- **Rol Interno:** Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el trabajo realizado.
- **Rol Externo:** Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

Según Hernández Pinto (2006) una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

- Seguridad Física
- Seguridad Lógica
- Seguridad en redes
- Seguridad en los recursos humanos
- Seguridad en el Outsourcing
- Planes de Contingencia

Documento de política de seguridad de la información

Según NTP ISO/IEC 27002 (2007) se debería establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento debería contener como mínimo la siguiente información:

a. Una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información.
b. El establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información.
c. Un marco para colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión del riesgo.
d. Una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la organización, por ejemplo:
    1) Conformidad con los requisitos legislativos y contractuales
    2) Requisitos de formación en seguridad
    3) Gestión de la continuidad del negocio
    4) Consecuencias de las violaciones de la política de seguridad
e. Una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad.
f. Las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

Esta política debería distribuirse por toda la organización, llegando hasta a todos los destinatarios en una forma que sea apropiada, entendible y accesible.

Las políticas de seguridad informática, también deben ofrecer:

- Explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos.
- Deberán establecer las expectativas de la organización, tales expectativas deben tener relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.
- Las políticas deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

G. Sistema de Gestión

Para Aguirre (2014) un sistema de gestión es una estructura probada para la gestión y mejora continua de políticas, procedimientos y procesos de una organización. La implementación de un sistema de gestión ayuda a mejorar la efectividad operativa, optimizar costos, lograr mejoras continuas, aumentar la satisfacción de las partes interesadas al negocio y renovar constantemente las estrategias de la organización.

H. Sistema de Gestión de Seguridad de la información

Los diferentes y constantes usos de las tecnologías de información en los negocios hacen que cada vez sea más fácil la expansión de éstos. Sin embargo, la cercanía y facilidad de éstos ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio.

Para contrarrestar dichas amenazas, las organizaciones deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación. La definición de SGSI se hace de manera formal en la norma ISO 27001, donde están los estándares y

mejores prácticas de seguridad de la información. (Ladino, Villa y López, 2011)

EL SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. (ISO/IEC 27001, 2005)

La implementación de un Sistema de Gestión de Seguridad de la Información permite establecer un proceso de mejora continua a través del seguimiento de un modelo PHVA (Planear, Hacer, Verificar, Actuar), para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información, con unas responsabilidades claras y el compromiso manifiesto por parte de directivas. (Prado Urrego, Caviedes, & Prado, 2012)

La ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio) (ISO 27000.es, 2005):

a. Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
b. Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
c. Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
d. Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
e. Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

f. Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

g. Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

h. Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

i. Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

I. Alcance de un SGSI

El SGSI cubre los siguientes niveles:

- Lógica: Confidencialidad, integridad y disponibilidad del software y datos de un SGI.
- Organizativa: Relativa a la prevención, detección y corrección de riesgos.
- Física: Protección de elementos físicos de las instalaciones: servidores, PCs, etc.
- Legal: Cumplimiento de la legislación vigente.

J. Implementación de un SGSI

Los siguientes pasos son expuestos por Robles y Rodriguez de Roa (2006), de modo sucinto y muy práctico:

PASO 1: Inicio del proyecto

En esta primera etapa se pretende asegurar para el éxito de todo el proyecto, el compromiso de la dirección general y seleccionar y formar a los miembros del equipo inicial del proyecto.

Para reducir la duración del proceso, el apoyo de la dirección debe estar presente a todos los niveles: operativo, técnico y presupuestario, así como en el de la planificación temporal. La dirección general debe comprender que su apoyo necesariamente

conlleva un esfuerzo continuo. La infraestructura establecida requerirá con toda seguridad ajustes, así como una mejora continua.

Respecto al equipo inicial del proyecto (coordinadores, grupos de trabajo, etc.), se debe formar un comité de dirección del proyecto que puede estar compuesto por un director ejecutivo, el director del proyecto y representantes de las diferentes unidades operativas implicadas. Es habitual que en algunas organizaciones grandes, el responsable de seguridad pueda llevar a cabo gran parte de las tareas del director del proyecto. En la mayoría de los casos, la implementación de la norma ISO 27001 en una organización requiere la implicación de todas las unidades operativas.

PASO 2: Alcance del SGSI

Definición del alcance del SGSI, etapa clave para el éxito posterior del proyecto:

- Alcance del SGSI: ¿qué unidades operativas y actividades estarán dentro del entorno de seguridad de la información?
- Limitaciones del SGSI: características específicas de la organización (tamaño, campo de acción, etc.), ubicación de la organización, activos (inventario de todos los datos críticos), tecnología.
- Conexiones o Interfaces: se deberán tener en cuenta por parte de la organización las relaciones con otros sistemas, otras organizaciones y proveedores externos.
- Requerimientos de Seguridad del SGSI: de naturaleza legal o del negocio.
- Exclusiones y justificación de las exclusiones (Declaración de aplicabilidad).
- Contexto estratégico: las medidas de seguridad planificadas deben tener en cuenta la posición actual y futura de la organización para alcanzar las metas fijadas por la dirección.
- Recopilación de la documentación existente: para simplificar y mejorar la eficacia del proceso desde el inicio, es necesaria una revisión de la documentación existente para evaluar el alcance de las medidas existentes, como el manual de gestión de calidad de la norma ISO 9001, el de la 14001 en su caso, o el manual de políticas de seguridad.
- Redacción de un inventario documental por los responsables de departamento (ejemplos):
    - Documentos de la política de seguridad.
    - Normas y procedimiento de las políticas (administrativos o técnicos).
    - Informes de evaluación de riesgos
    - Planes de tratamiento de riesgos.

- Documentos que indiquen la existencia de controles de seguridad y su gestión; por ejemplo, informes y planes de auditoría, informes de incidencias, etc.

PASO 3: Evaluación de riesgos

Con independencia del tipo o tamaño de la empresa, todas las organizaciones son vulnerables a las amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información importante.

Cuanto antes se adopten las medidas correctivas, la seguridad representará un menor coste y será más efectiva. Para poder realizar una identificación y selección de controles más sencillos que permitan una mejor gestión de los recursos humanos y financieros se debe conocer la fuente y naturaleza de las amenazas.

- Aplicabilidad de los controles de la ISO 17799: diagnóstico preliminar.
- Identificación y evaluación de activos, datos a proteger.
- Identificación y evaluación de amenazas y vulnerabilidades.

PASO 4: Tratamiento y administración del riesgo

En este paso es básico conocer cómo la selección y la implantación de los controles permiten reducir los riesgos a un nivel aceptable por la organización. Esta gestión generalmente es una función de la:

- Política de seguridad inicial.
- Nivel de seguridad requerido.
- Resultados de la evaluación de riesgos.
- Reglamentación y legislación aplicable.
- Regulaciones y restricciones del negocio existentes.

En general existen cuatro opciones para el tratamiento del riesgo: reducir el riesgo, aceptar el riesgo, evitar el riesgo y transferencia del riesgo.

PASO 5: Programa de Formación y Sensibilización para el Personal

La organización debe asegurarse de que todos los miembros del personal con responsabilidades específicas en el SGSI están debidamente formados, cualificados y capacitados para realizar sus funciones. La organización debe también asegurarse de que el personal necesario está concienciado de la importancia de sus

actividades en la seguridad de la información y de cómo contribuyen ellos a alcanzar los objetivos del SGSI.

Es importante desarrollar un programa de formación y sensibilización con el fin de “educar” a todos los empleados. Los empleados tienen que entender y respetar las buenas prácticas de seguridad de la información.

PASO 6: Documentación e implantación del SGSI

La documentación de un SGSI es una exigencia necesaria y previa a la implantación del sistema y se articula en torno a dos puntos estratégicamente claves:

- La descripción de la estrategia de la organización, sus objetivos, la evaluación de riesgos y las medidas adoptadas para evitar o atenuar los mismos.
- El control y el seguimiento del funcionamiento del SGSI. Es usual plantear por lo menos cuatro niveles de documentación.

Una vez realizado lo anterior, o en paralelo, se lleva a cabo la implantación de los documentos creados y se complementa con la formación del personal en las etapas en que sea necesario.

PASO 7: Ajustes y preparación para la Auditoría de Certificación

El Diagnóstico es uno de los pasos “previos e imprescindibles” de toda organización que desee y tenga como objetivo la certificación de acuerdo a la norma ISO 27001, con el fin de validar si el sistema sigue las especificaciones necesarias para la implantación de su marco de gestión.

Este documento (que se convertirá en un registro imprescindible del SGSI de cara a la auditoría de certificación) proporciona la justificación para la aplicabilidad o no aplicabilidad de cada control ISO 27001 del SGSI en cuestión, incluyendo también dónde es aplicable el estado de implantación de cada control.

PASO 8: Control y mejora continua

Control y mejora continua del SGSI de acuerdo al Ciclo de DEMING (P-D-C-A) establecido en la norma debiéndose realizar antes de la Auditoría de Certificación en función de los resultados del diagnóstico.

2.2.2. Gestión de Riesgo

Alcántara Torres (2015) nos dice que la gestión de riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo, es así que tenemos a los siguientes parámetros como son los que detallaremos a continuación:

1. Análisis del Riesgo: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
2. Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
3. Reducción: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
4. Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sancionar el incumplimiento.

Para lograr el éxito de la gestión de riesgo, es vital tener en cuenta tanto la cultura como la estructura de la organización, la misión y los objetivos de negocio que se hayan trazado, la definición de los procesos organizacionales y el conocimiento de marcos de buenas prácticas generalmente aceptados. (Huamán Monzón, 2014)

En el escenario que una amenaza se materialice, la gestión de riesgos garantizara que el impacto que se tendrá internamente (en la organización) será manejable, es decir, que estará dentro de los límites de costos aceptables sin perturbar la continuidad del negocio. (Huamán Monzón, 2014)

Sabemos que en toda actividad empresarial hay riesgo (cuando hacemos algo o cuando dejamos de hacer algo), la gestión de Riesgos debe brindar garantía de seguridad en cualquier actividad que emprenda la institución apoyándose en la estrategia de seguridad que ésta esté llevando a cabo. (Huamán Monzón, 2014)

Figura N° 16. Fases de Gestión de Riesgos
Fuente: (Huamán Monzón, 2014)

A. Proceso de Gestión de Riesgos

Costas Santos (2011) Establece que la gestión de los riesgos permite tener control sobre el desarrollo, la implementación y funcionamiento de los procesos, lo cual llevara a lograr de manera eficiente el cumplimiento de sus objetivos estratégicos y estar preparados para enfrentar cualquier incidente que pueda presentarse.

Sobre los procesos, se construyen controles con el objetivo de reducir la frecuencia de las amenazas o limitar el daño causado y llevar el nivel de riesgo a un nivel aceptable por la organización.

Dependiendo del tipo de riesgo, se puede optar por:

- Evitar el riesgo: por ejemplo eliminando el activo.
- Mitigar el riesgo: implementando controles para reducir la probabilidad y el impacto.
- Transferir el riesgo: por ejemplo contratando un seguro con cobertura para ese riesgo. Aceptar el riesgo: reconociendo que el riesgo existe y monitorizarlo.

Según la NTP-ISO/IEC 27005 (2009), el proceso de gestión del riesgo en seguridad de la información consiste en establecer el contexto, evaluar el riesgo, tratar el riesgo, aceptar el riesgo, comunicar el riesgo y monitorear y revisar el riesgo.

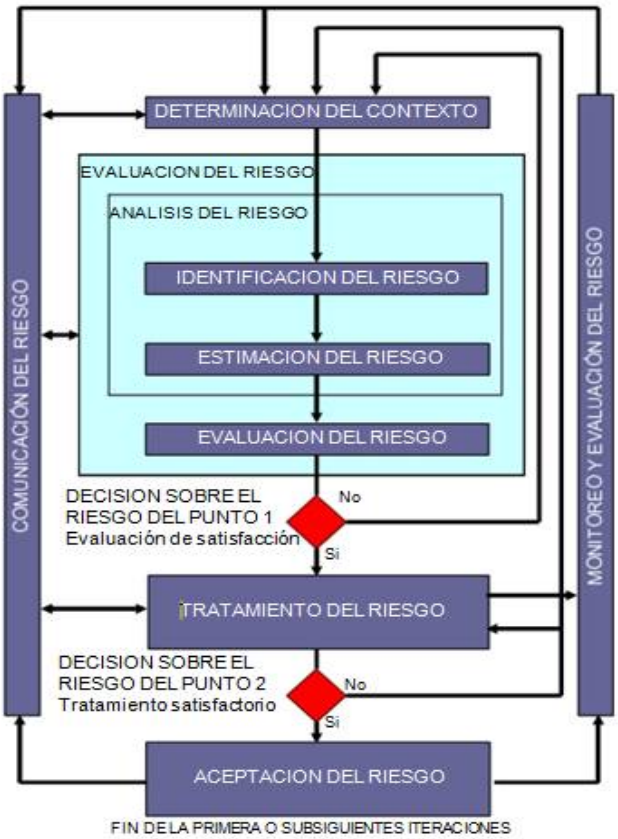


Figura N° 17. Proceso de gestión del riesgo de seguridad de la información
Fuente: (NTP-ISO/IEC 27005, 2009)

Tal como lo ilustra la figura anterior, el proceso de gestión de seguridad de la información puede ser iterativo para la evaluación del riesgo y/o para las actividades de tratamiento del riesgo. Un enfoque iterativo para la conducción de la evaluación del riesgo puede incrementar la profundidad y detalle de la evaluación en cada iteración. El enfoque iterativo provee un buen balance entre minimizar el tiempo y el esfuerzo que se emplea en identificar los controles y a la vez asegurar que se evalúe apropiadamente los altos riesgos.

Primero se determina el contexto. Luego se realiza una evaluación del riesgo. Si esto provee suficiente información para determinar efectivamente las acciones requeridas para modificar los riesgos a un nivel aceptable, entonces la tarea está completa y sigue el tratamiento del riesgo. Si la información es suficiente, se conducirá otra iteración de la evaluación del riesgo con el contexto revisado (por ejemplo criterios de evaluación del riesgo, criterios de aceptación del riesgo o criterios de impacto) posiblemente en partes limitadas del alcance total.

La eficacia en el tratamiento del riesgo depende de los resultados de la evaluación del riesgo. Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel aceptable de riesgo

residual. En esta situación, podría requerirse otra iteración de la evaluación del riesgo con parámetros de contexto cambiados (por ejemplo evaluación del riesgo, aceptación del riesgo o criterios de impacto), si fuera necesario, seguido de otro tratamiento del riesgo.

La actividad **de aceptación del riesgo** tiene que asegurar que los gerentes de la organización acepten explícitamente los riesgos residuales. Esto es especialmente importante en una situación donde la implementación de controles se omite o pospone, por ejemplo debido al costo.

Durante todo el proceso de gestión del riesgo en seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los gerentes apropiados y al personal operativo. Incluso antes del tratamiento de los riesgos puede ser muy valioso contar con información sobre los riesgos identificados para administrar los incidentes y puede ayudar a reducir el daño potencial. La conciencia de los gerentes y el personal respecto de los riesgos, la naturaleza de los controles empleados para mitigar los riesgos y las áreas de preocupación para la organización ayudan a tratar los incidentes y los eventos inesperados de la manera más eficaz.

El Sistema de Gestión de Seguridad de la Información específica que los controles implementados dentro del alcance, límites y contexto deben basarse en el riesgo. La aplicación de un proceso de gestión del riesgo en seguridad de la información puede satisfacer este requisito.

En un SGSI, determinar el contexto, evaluar el riesgo, desarrollar un plan de tratamiento del riesgo y aceptar el riesgo son parte de la fase del "**plan**". En la fase de "**hacer**" del Sistema de Gestión de Seguridad de la Información, se implementan las acciones y controles requeridos para reducir el riesgo a un nivel aceptable de acuerdo con el plan de tratamiento del riesgo. En la fase de "**verificar**" del Sistema de Gestión de Seguridad de la Información, los gerentes determinarán la necesidad de revisiones de la evaluación del riesgo y el tratamiento del riesgo a la luz de los incidentes y cambios en las circunstancias. En la fase de "**actuar**", se realizan todas las acciones requeridas, incluyendo la aplicación adicional del proceso de gestión del riesgo en seguridad de la información.

La tabla siguiente resume las actividades de gestión del riesgo en seguridad de la información relevantes a las cuatro fases del proceso del Sistema de Gestión de Seguridad de la Información:

Tabla N° 25. Alineamiento del SGSI y del Proceso de Gestión del Riesgo en Seguridad de la Información

Proceso Sistema de Gestión de Seguridad de la información	Proceso de Gestión del Riesgo en Seguridad de la Información
Plan	Determinar el contexto. Evaluar el riesgo. Desarrollar el plan de tratamiento del riesgo. Aceptar el riesgo.
Hacer	Implementar el plan de tratamiento del riesgo.
Verificar	Monitoreo y revisión continuos de los riesgos.
Actuar	Mantener y mejorar el Proceso de Gestión del Riesgo en Seguridad de la Información.

Fuente: Elaboración propia adaptado del Resultado del Cuestionario NTP ISO/IEC 27002:2005

2.2.3. Ciclo de Deming

Es evidente que la seguridad de la información no se termina en la implementación de un "firewall" o con la contratación de una empresa de seguridad. Es necesario integrar las múltiples iniciativas puestas en ejecución dentro de una estrategia global con el fin de que cada elemento ofrezca un nivel óptimo de protección. Es a este nivel que intervienen los sistemas de gestión de la seguridad de la información permitiendo coordinar los esfuerzos para alcanzar una seguridad óptima. (Robles & Rodriguez de Roa, 2006)

Un sistema de gestión debe incluir un método de evaluación, medidas de protección y un proceso de documentación y de revisión. Esto último es el principio del Modelo del PDCA (Establecer-Implantar-Monitorizar y Verificar Actuar, manteniendo y mejorando el SGSI). Este modelo popularizado por W.Edwards Deming (y conocido como el "Ciclo Deming") recuerda fuertemente al modelo de gestión de la calidad ISO 9001 (ver figura N° 06). (Robles & Rodriguez de Roa, 2006)

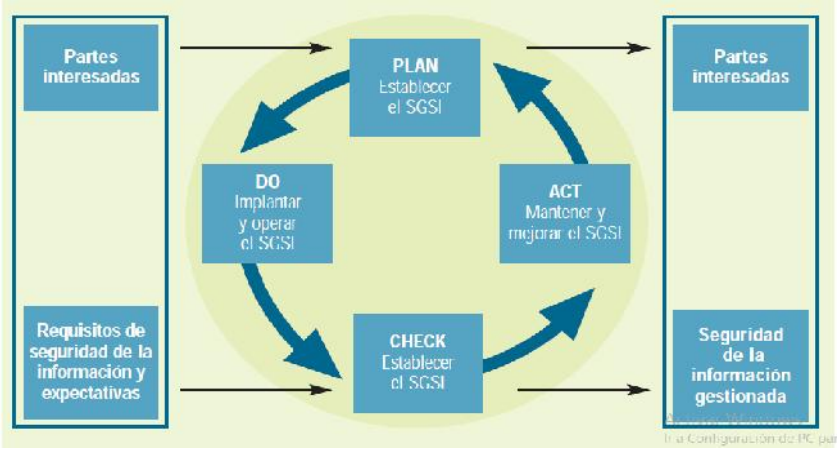


Figura N° 18. Ciclo Deming
Fuente: (Robles & Rodriguez de Roa, 2006)

- PLAN. En esta fase necesaria para la planificación, definición y el establecimiento del SGSI, es importante considerar el entorno de la actividad de la organización que implementará el Sistema. Se deberían identificar, por ejemplo, directrices corporativas aplicables y requisitos legales. Además de esto, el contexto de la actividad de la organización debería quedar reflejado en las políticas y objetivos de seguridad y se debería considerar al definir el alcance del SGSI. Durante esta fase la organización también diseña un procedimiento formal para la continua identificación y evaluación de riesgos y la selección de los objetivos de control y controles que le permitirán gestionar estos riesgos. Al final de este proceso, la organización prepara la declaración de aplicabilidad.

- DO. Hacer, implementar. Es importante centrarse inicialmente en el desarrollo e implementación de un plan efectivo y a medio y largo plazo para la atenuación de los riesgos. Durante esta fase, los controles seleccionados en la fase de planificación se implementarán para alcanzar los objetivos de control. En esta fase se inicia el Plan de Formación para incrementar la concienciación y conocimiento del personal que garantice la correcta implementación de los controles.

- CHECK. Seguimiento, monitorización y revisión del SGSI. Realización periódica de auditorías internas del SGSI y seguimiento regular de la eficiencia del sistema.

- ACT. Actuar, mantener y mejorar el SGSI. Cuando se han identificado las vulnerabilidades y debilidades, se deben llevar

a cabo las medidas correctivas y preventivas apropiadas para mejorar el SGSI, así como las planificaciones temporales de estas mejoras.

Así mismo como hemos mencionado anteriormente que el cronograma de implementación incremental del SGSI, propuesto por la ONGEI, el cual se basa en 5 fases toma como referencia el ciclo de DEMING.

Tabla N° 26. Relación entre el cronograma de implementación incremental de un SGSI de la ONGEI y el círculo de Deming

CRONOGRAMAL DE SGSI PROPESTO POR LA ONGEI		
FASE	**NOMBRE**	**RELACION CON EL CIRCULO DE DEMING**
I	ORGANIZACIÓN	PLANEAR – PLAN
II	PLANIFICACION	
III	DESPLIEGE	HACER – DO
IV	REVISION	REVISAR – CHECK
V	CONSOLIDACIÓN	ACTUAR – ACT

Fuente: (Portal Oficial de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI, NTP ISO/IEC 27001:2008)

2.2.4. Marcos de referencia

A. ISO/IEC 27000

La serie de normas ISO/IEC 27000 se denomina “Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)”, proporciona un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias:

- Sistema de gestión de la seguridad de la información.
- Valoración de riesgos.
- Controles.

La norma técnica ISO/IEC 27000 está enfocada en procesos, toda la organización se ve involucrada en su implementación en lo que a cada una le corresponde de tal manera que la suma de cada uno de los esfuerzos individuales, apoyados por la gestión y dirección de las personas que lideran el proceso, termine formando un SGSI

que logre ejecutar todas las actividades de administración de riesgos incluyendo la creación de medidas ante tales riesgos y los controles para evaluar la efectividad de tales medidas. (Reina García & Morales Ramírez , 2014)

La familia de normas ISO/IEC 27000 son de aplicación voluntaria pero su uso a nivel mundial facilita las relaciones comerciales entre compañías internacionales y aumenta la competitividad en el mercado, también ayuda a mejorar la calidad y productos ofrecidos ya que este estándar internacional provee un modelo para establecer, implementar, operar y mantener un SGSI basado en los objetivos de la compañía, requisitos, requerimientos y expectativas de seguridad independiente del tamaño, estructura y razón de ser del negocio. (Reina García & Morales Ramírez , 2014)

ISO/IEC 27000 contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. (Reina García & Morales Ramírez , 2014)

En nuestra investigación las normas de la familia ISO 27000, que utilizaremos serán las siguientes:

a. **ISO/IEC 27001 – Sistema de Gestión de la Seguridad de la Información**

   Es la norma principal de la serie ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002.

   Este estándar brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación. (Aguirre Mollehuanca, 2014)

   Este estándar internacional “proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información dentro de cualquier organización“. (ISO/IEC 27001, 2005)

   Indica las acciones que tiene que realizar una organización para poder alinearse a los requerimientos que tiene un SGSI. Para todos los procesos dentro del SGSI, la norma se basa en

el modelo Plan-Do-Check-Act, el cual toma como input las expectativas que las partes interesadas de la organización tienen con respecto a la seguridad de información y, siguiendo este plan PDCA, produce un output de seguridad de información que satisfacen aquellas expectativas.

La ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un SGSI. Estos requerimientos describen el comportamiento previsto de un SGSI una vez que es completamente operacional. El estándar no es una guía paso a paso sobre cómo construir o crear un SGSI. (BSI Group México , s/a)

b. ISO/IEC 27002 - Código de prácticas para los controles de seguridad de la información

Esta norma internacional proporciona directrices para normas organizacionales de seguridad de la información y para las prácticas de gestión de seguridad de la información. Incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta los riesgos del entorno de seguridad de la información de la organización. (ISO/IEC 27002, 2013)

La ISO/IEC 27002 (2013) está diseñada para ser utilizada por las organizaciones que pretenden:

- Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de seguridad de la Información basado en la Norma ISO/IEC 27001.
- Implementar los controles de seguridad de la información comúnmente aceptados;
- Desarrollar sus propias directrices de gestión de seguridad de la información.

Esta norma nos muestra una serie de controles que buscan mitigar el impacto de ocurrencia de los diferentes riesgos que se expone una organización. (ISO/IEC 27002, 2013)

La ISO/IEC 27002 (2013) presenta 14 dominios, 35 objetivos de control y 114 controles. Los 14 dominios mencionados previamente son:

- Dominio 1: Políticas de seguridad
- Dominio 2: Organización de la seguridad
- Dominio 3: Seguridad de recursos humanos
- Dominio 4: Gestión de activos
- Dominio 5: Control de acceso lógico
- Dominio 6: Cifrado

- Dominio 7: Seguridad física y ambiental
- Dominio 8: Seguridad en las operaciones
- Dominio 9: Seguridad en las telecomunicaciones
- Dominio 10: Adquisición, desarrollo y mantenimiento de los sistemas de información
- Dominio 11: Relaciones con los suministradores
- Dominio 12: Gestión de incidentes
- Dominio 13: Aspectos de la SI en la continuidad del negocio
- Dominio 14: Cumplimiento

c. ISO/IEC 27003 - Tecnología de la información - Técnicas de seguridad - Orientación para la implementación de un sistema de gestión de la seguridad de la información.

ISO 27003 es un estándar internacional que constituye una guía para la implantación de un SGSI. Se trata de una norma adaptada tanto para los que quieren lanzarse a implantar un SGSI como para los consultores en su trabajo diario, debido a que resuelve ciertas cuestiones que venían careciendo de un criterio normalizado. (ISOTools Excellence, 2014)

ISO 27003 focaliza su atención en los aspectos requeridos para un diseño exitoso y una buena implementación del Sistema de Gestión de Seguridad de la Información – SGSI – según el estándar ISO 27001. Contiene una descripción del proceso de delimitación del SGSI, y además el diseño y ejecución de distintos planes de implementación. (ISOTools Excellence, 2014)

La norma tiene el siguiente contenido:

1. Alcance.
2. Referencias Normativas.
3. Términos y Definiciones.
4. Estructura de esta Norma.
5. Obtención de la aprobación de la alta dirección para iniciar un SGSI.
6. Definición del alcance del SGSI, límites y políticas.
7. Evaluación de requerimientos de seguridad de la información.
8. Evaluación de Riesgos y Plan de tratamiento de riesgos.
9. Diseño del SGSI.

- Anexo A: lista de chequeo para la implementación de un SGSI.

- Anexo B: Roles y responsabilidades en seguridad de la información
- Anexo C: Información sobre auditorías internas.
- Anexo D: Estructura de las políticas de seguridad.
- Anexo E: Monitoreo y seguimiento del SGSI.

d. ISO/IEC 27005 EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información

ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001. (ISOTools Excellence, 2014)

ISO 27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia organización. Los usuarios elijen el método que mejor se adapte para, por ejemplo, una evaluación de riesgos de alto nivel seguido de un análisis de riesgos en profundidad sobre las zonas de alto riesgo. (ISOTools Excellence, 2014)

En el Anexo E de la norma, se detallan los Enfoques de evaluación del riesgo en seguridad de la información. La NTP-ISO/IEC 27005 (2009) muestra dos enfoques:

E.1 Evaluación del riesgo en seguridad de la información de alto nivel (NTP-ISO/IEC 27005, 2009)

Las características de la iteración de la evaluación del riesgo del alto nivel pueden incluir las siguientes:

- La evaluación del riesgo de alto nivel puede dirigirse a una visión más global de la organización y de sus sistemas de información, considerando los aspectos de la tecnología como independientes de las cuestiones empresariales. Al hacer esto, el análisis del contexto se concentra más en el negocio y el entorno operativo que en los elementos tecnológicos.

- La evaluación del riesgo de alto nivel puede resolver una lista más limitada de amenazas y vulnerabilidades agrupadas en dominios definidos o para hacer el proceso más expeditivo, puede centrarse en los escenarios de riesgo o ataque en vez de sus elementos.
- Los riesgos que se presentan en una evaluación del riesgo de alto nivel frecuentemente son dominios de riesgo más generales que los riesgos específicos identificados.

Las ventajas de una evaluación dl riesgo de alto nivel son las siguientes:

- La incorporación de un enfoque simple inicial probablemente gane aceptación del programa de evaluación del riesgo.
- Debe ser posible construir una imagen estratégica de un programa de información organizacional, es decir actuara como una buena ayuda a la planificación.
- Como los análisis de riesgo inicial están en un alto nivel y son potencialmente menos exactos, la única desventaja potencial es que pueda no identificarse que algunos procesos o sistemas no empresariales requieren una segunda evaluación detallada del riesgo. Esto se puede evitar si existe una información adecuada sobre todos los aspectos de la organización y su información y sistemas, incluyendo información adquirida a partir de la evaluación de incidentes de seguridad de la información.

Una regla general que debe aplicarse es si la falta de seguridad en la información puede resultar en consecuencias adversas significativas para la organización, sus procesos empresariales o sus activos, luego se hace necesaria una segunda iteración de la evaluación del riesgo a nivel más detallado para identificar los riesgos potenciales.

E.2 Evaluación detallada del riesgo en seguridad de la información (NTP-ISO/IEC 27005, 2009)

El proceso de evaluación detallada del riesgo en seguridad de la información incluye una identificación y valorización profunda de los activos, la evaluación de amenazas a esos activos y la evaluación de vulnerabilidades. Los resultados de esas actividades se utilizan entonces para evaluar los riesgos y luego identificar el tratamiento del riesgo.

Se puede evaluar las consecuencias de varias maneras, incluyendo el uso de medidas cuantitativas, por ejemplo monetarias, y cualitativas (las que se pueden basar en el uso de adjetivos como moderado o grave), o una combinación de ambas.

B. Metodología MAGERIT para Análisis de Riesgos

Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (Magerit, 2012)

Magerit, tiene como uno de sus principales objetivos, el ofrecer un método para analizar los riesgos y ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. (Espinoza Aguinaga, 2013)

El análisis de riesgos propuesto por MAGERIT es una aproximación metódica que permite determinar el riesgo siguiendo los siguientes pasos:

- Determinar los activos relevantes para la empresa.
- Determinar las amenazas a la que están expuestos aquellos activos.
- Estimar el impacto, definido como el daño sobre el activo, si se llega a concretar la amenaza.
- Valorar dichos activos en función del coste que supondría para la empresa recuperarse ante un problema de disponibilidad, integridad o confidencialidad de información.
- Valorar las amenazas potenciales.
- Estimar el riesgo.

Esta metodología propone para el análisis de riesgos las 4 etapas siguientes:

- La etapa 1, Planificación del análisis y gestión de riesgos, establece las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos.

- La etapa 2, Análisis de riesgos, permite identificar y valorar las entidades que intervienen en el riesgo.
- La etapa 3, Gestión de riesgos, permite identificar las funciones o servicios de salvaguarda reductores del riesgo detectado.
- La etapa 4, Selección de salvaguardas, permite seleccionar los mecanismos de salvaguarda que hay que implementar.

III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Descripción de la metodología

En esta sección se describe la metodología propuesta que servirá de guía para la implementación del Sistema de Gestión de Seguridad de la Información para el CGT, aunque no es parte del alcance de la presente investigación el establecer una metodología para la implementación de un SGSI, se dio la necesidad de establecer un modelo propuesto para la implementación de lo establecido en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 para el CGT, tomando como referencia los siguientes marcos normativos:

- NTP ISO/IEC 27001
- NTP ISO/IEC 27002
- NTP ISO/IEC 27003
- NTP ISO/IEC 27005
- Metodología MagerIT

Este modelo de implementación del SGSI propuesto se basa en la estructura que propone la NTP ISO/IEC 27003:2012, la cual es una norma que provee una guía práctica en el desarrollo del plan de implementación de un Sistema de Seguridad de la Información dentro de una organización de acuerdo con la Norma Técnica Peruana NTP-ISO/IEC 27001.

La norma NTP ISO/IEC 27003:2012, explica la implementación de un SGSI enfocándose en la iniciación, planificación y definición del proyecto, esta norma no cubre las actividades de operación y otras actividades del SGSI, sino que abarca los conceptos sobre diseñar las actividades que tendrán lugar después de que comiencen las operaciones del SGSI propuesto para el CGT.

A partir de ello, se elaboró un marco metodológico, compuesto por tres fases, tal como se muestre en la Tabla N° 27: Marco Metodológico Propuesto:

- **Fase I - Establecimiento del SGSI:**

  En esta fase se desea obtener la aprobación de la Gerencia (Fase I de la Norma NTP ISO/IEC 27003:2012).

  Se iniciará el proyecto de SGSI en el CGT mediante la definición de un caso de negocio y plan del proyecto, con el objetivo de que la Alta dirección del CGT entienda la importancia de un SGSI, y aclarar las funciones y responsabilidades de seguridad de la información dentro del CGT que requiere un proyecto de SGSI.

- **Fase II – Planeamiento del SGSI:**

  En esta fase se define las siguientes actividades:

  - DEFINIR EL ALCANCE, LÍMITES Y POLÍTICA DEL SGSI (Fase II de la Norma NTP ISO/IEC 27003:2012): El Objetivo de esta fase es definir detalladamente el alcance y los límites del SGSI y desarrollar la política del SGSI, obteniendo el aval de la dirección.
  - REALIZAR UN ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN (Fase III de la Norma NTP ISO/IEC 27003:2012): El Objetivo de esta fase es definir los requerimientos relevantes a ser soportados por el SGSI, identificar los activos de información y obtener el estado actual de la seguridad dentro del alcance.
  - REALIZAR UNA EVALUACIÓN DEL RIESGO Y PLANIFICAR EL TRATAMIENTO DEL RIESGO (Fase IV de la Norma NTP ISO/IEC 27003:2012): El Objetivo de esta fase es definir la metodología de evaluación del riesgo, identificar, analizar y evaluar los riesgos de seguridad de información para seleccionar las opciones de tratamiento del riesgo y seleccionar los objetivos de control y los controles.

- **Fase III – Verificación del SGSI:**

  Esta fase pretende verificar si el desarrollo del plan de implementación del Sistema de Gestión de Seguridad de la Información propuesto considera los puntos descritos en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Así mismo, en el Diagrama de Implementación del Sistema de Gestión de Seguridad de la Información, se muestra las actividades del marco metodológico en forma secuencial, las salidas de algunas de ellas y los marcos normativos utilizados.

Tabla N° 27. Marco Metodológico Propuesto

MARCOS DE REFERENCIA

NTP-ISO/IEC 27001:2014

EDI. Tecnología de la información. Técnicas de seguridad. Sistema de Gestión de la información - Requisitos.

NTP ISO/IEC 17799:2007 Y ISO/IEC 27002:2013

EDI. Tecnología de la información. Código de Buenas Prácticas para la Gestión de la información.

NTP ISO/IEC 27003:2012

EDI. Tecnología de la información. Directrices para la implementación de un sistema de gestión de la seguridad de la información.

NTP ISO/IEC 27005:2009

EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información.

Se tomó como referencia:

- procesos.

Capability Maturity Model (CMM)

Se tomó como referencia:

- Niveles de Madurez de capacidad de los procesos.

Metodología MagerIT

Se tomó como referencia:

- Clasificación de activos
- Clasificación de amenazas
- Clasificación de controles
- Tablas de valoración de los componentes del SGSI

METODOLOGIA

ESTABLECIMIENTO DEL SGSI

a. Obtener aprobación de la Dirección para la implementación del SGSI:
   - Caso de Negocio.
   - Plan de proyecto propuesto.
   - Aprobación de la Dirección para iniciar un proyecto para implementar un SGSI.

PLANEAMIENTO DEL SGSI

a. Definir alcance y Política de Seguridad de la Información.
b. Realizar el análisis de la Organización.
   - Descripción de los principales procesos de la organización.
   - Identificación de los activos de información de los principales procesos de la organización.
c. Realizar evaluación del riesgo y selección de las opciones de tratamiento de riesgo.
   - Definir y aplicar un proceso de evaluación de riesgo de la Seguridad de la Información.
   - Definición del alcance y límites del proceso de Gestión del riesgo en SI.
   - Identificación, valorización de activos y evaluación de impacto.
   - Análisis y evaluación del riesgo en SI
   - Identificación y evaluación de las opciones para el tratamiento del riesgo en SI.
   - Aceptación del riesgo en SI.
   - Comunicación del riesgo en SI
   - Selección de Objetivos de control para el tratamiento de riesgos.
   - Preparar enunciado de aplicabilidad (SOA)

VERIFICACIÓN DEL SGSI

a. Verificación de los puntos descritos en la NTP ISO/IEC 27001:2014

Fuente: Desarrollo Propio

Diagrama de Implementación del Sistema de Gestión de Seguridad de la Información

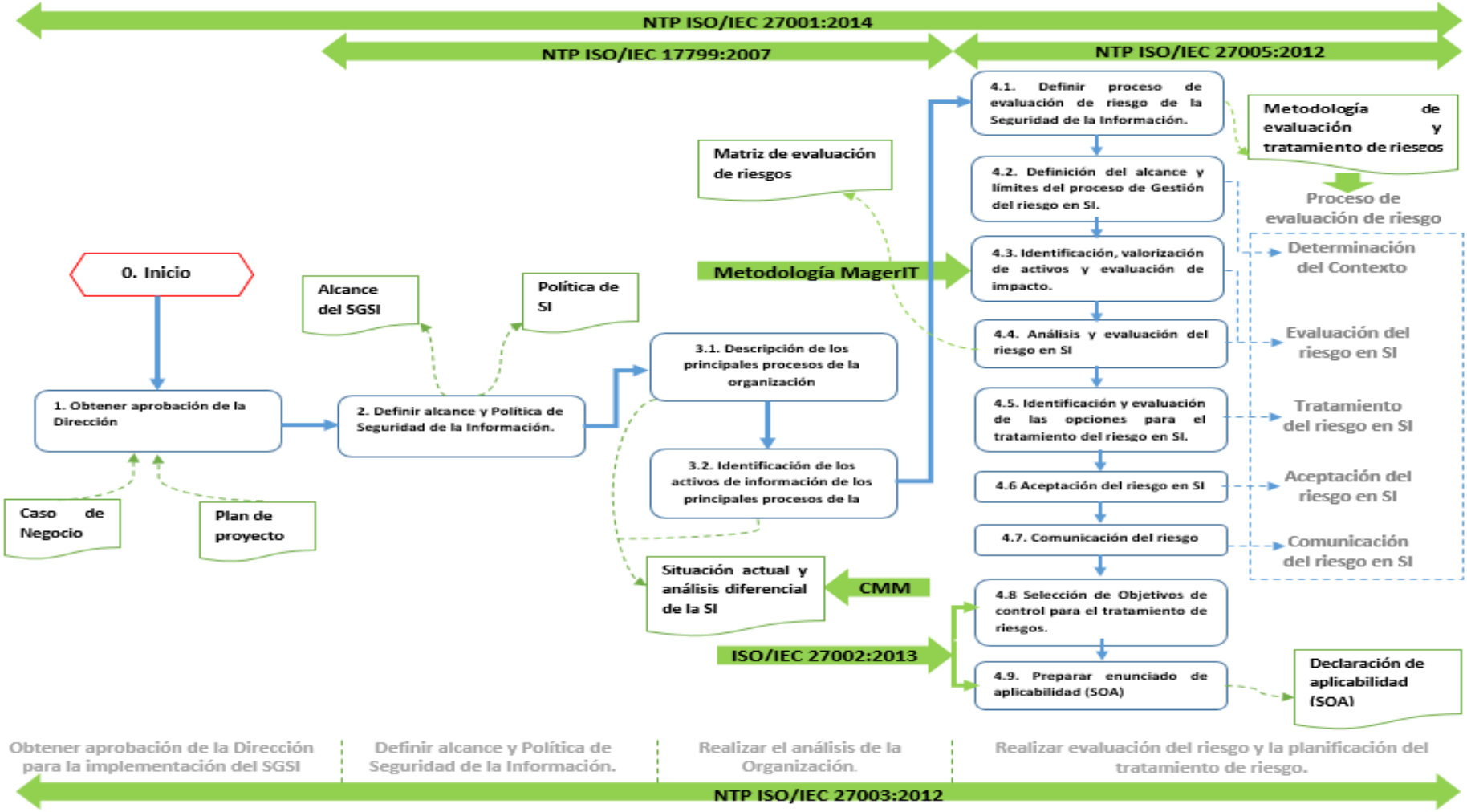


Figura N° 19. Diagrama de Implementación del Sistema de Gestión de Seguridad de la Información
Fuente: Desarrollo Propio

3.2. Establecimiento del SGSI

3.2.1. Obtener la aprobación de la Organización

Con el fin de obtener el apoyo y la aprobación de la alta dirección del CGT para la implementación del Sistema de gestión de Seguridad de la Información es necesario presentarles dos documentos importantes, los cuales expliquen el grado de importancia de implementar este tipo de proyecto a la institución así como los plazos, las funciones y responsabilidades del mismo. Estos documentos son el caso de negocio y plan de proyecto.

a) Caso del negocio

El Caso de Negocio presentado a continuación tiene por finalidad obtener el total apoyo de la alta dirección del CGT ya que es crucial para el desarrollo del proyecto. Adicionalmente, la NTP ISO/IEC 27001 indica que se debe buscar obtener este compromiso dentro de la fase inicial del proceso de implementación. Ante esta situación, se desarrolló un documento que permita evidenciar ante la gerencia del CGT la necesidad de implementar un SGSI, el cual incluirá una descripción del CGT, el alcance preliminar, los objetivos y beneficios de un SGSI para la institución, roles y responsabilidades en la seguridad de la información, así como también cronograma con hitos claves, costos de implementación de una manera general, alcance y limitaciones del proyecto.

Cabe destacar que el modelo utilizado para la creación del presente Caso de Negocio es tomado en cuenta de la norma NTP ISO/IEC 27003, el cual establece una serie de secciones recomendadas más no mandatorias, siendo parte del proceso la elección de las secciones que sean pertinentes para el caso específico que se desea presentar.

b) Plan del proyecto

El plan del proyecto para la implementación del Sistema de Gestión de Seguridad de la Información tiene como objetivo definir los documentos que se redactarán (entregables del proyecto), los plazos, las funciones y responsabilidades del proyecto.

El Jefe de Tecnología de la Información y el Gerente de la Oficina General de Administración son quienes verificaran el Plan del Proyecto de SGSI junto con el Caso de Negocio para luego ser presentado a la Gerencia del CGT para su aprobación.

El fin de que aprueben ambos documentos se logró un compromiso total del CGT e iniciar la ejecución del proyecto del SGSI.

Así mismo los beneficios esperados del compromiso de la Gerencia del CGT para implementar un SGSI son:

a) Conocimiento e implementación de leyes, regulaciones, obligaciones y normas pertinentes relacionadas con la seguridad de la

información, que permitan evitar responsabilidades y multas en razón del incumplimiento.

b) Uso eficiente de múltiples procesos para la seguridad de la información.

c) Identificación y protección de la información crítica del CGT.

3.2.2. Planeamiento del SGSI

A. Alcance y Políticas de SI

Alcance del SGSI

El CGT para establecer el alcance del SGSI debe determinar los límites y la aplicabilidad del mismo, para ello se planteó que el Sistema de Gestión de Seguridad de la Información cubrirá solo doce dominios de la norma NTP-ISO/IEC 27001 con la finalidad de salvaguardar la información, sistemas de información, procesos y personas del CGT, siendo estos:

1. A.5. Política de seguridad de la Información
2. A.6. Organización de la seguridad de la información
3. A.7. Seguridad en Recursos Humanos
4. A.8. Gestión de activos
5. A.9. Control de acceso
6. A.11. Seguridad física y ambiental
7. A.12. Seguridad de las operaciones
8. A.13. Seguridad en las comunicaciones
9. A.14. Adquisición, desarrollo y mantenimiento de sistemas de información
10. A.16 Gestión de incidentes en la seguridad de información
11. A.17 Aspectos de seguridad de información en la gestión de continuidad del negocio
12. A.18 Cumplimiento

Así mismo para validar el alcance del SGSI se debe alinear con lo que exige la NTP ISO/IEC 27001 lo cual es:

"*Cuando se determina este alcance la organización debe considerar:*

a. *Lo aspectos externos e internos referido en 4.1 (**Comprender la organización y su contexto**)*
b. *Los requisitos referidos en 4.2 (**Comprender las necesidades y expectativas de las partes interesadas**)*
c. *Las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones."* (NTP-ISO/IEC 27001, 2014)

En el punto "**Comprender la organización y su contexto**", se hizo un análisis de todo el CGT y de toda la información disponible y se clasifico en:

- Marco estratégico institucional: Se muestra una información general del CGT propia del Plan estratégico Institucional 2014 – 2018.
- Marco situacional general: Para el desarrollo del contexto interno y externo de la institución, se muestra el Análisis FODA del CGT.
- Diagnostico Institucional: Se muestra la estructura y organización del CGT, así como todos los documentos de gestión que posee.

Toda esta información puede ser visualizada en su totalidad dentro del capítulo "Características claves de la organización (su función, estructura, servicios, etc.)" del Documento Alcance del SGSI del CGT

En el punto "**Comprender las necesidades y expectativas de las partes interesadas**" se identificaron las siguientes partes interesadas frente al SGSI y sus requerimientos:

Tabla N° 28. Partes interesadas frente al SGSI

PARTES INTERESADAS	REQUERIMIENTOS
Entes de control (Control Interno)	Cumplimiento de la legislación y regulación en temas relativos a seguridad de la información referente a las actividades del CGT.
Comunidad del distrito	Protección de las operaciones y servicios que ofrece el CGT al igual que la información que brinda.
Alta dirección	Contar con altos estándares de seguridad para el desarrollo de las operaciones y servicios para así fortalecer la imagen del CGT en el distrito.
Áreas operativas del CGT	Contar con altos estándares de seguridad para el desarrollo de sus actividades, como también proteger los activos de información que utilizan en sus operaciones.
Administrativos y colaboradores	Contar con condiciones de seguridad física y lógica en el desarrollo de sus funciones dentro del CGT, sin sentir vulnerados sus derechos de privacidad.

Fuente: Desarrollo Propio

En el punto "**Las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones**", para ello es necesario definir que procesos o áreas del CGT formaran parte del alcance del SGSI.

En este punto no es necesario abarcar toda la institución, es más, es recomendable empezar con un alcance limitado, en el que se involucren los procesos críticos del CGT o que contengan la información más relevante para la institución.

Política de seguridad de la información

Se deben definir la política de seguridad de la Información con el objetivo de proteger los recursos de información del CGT y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información.

Para la redacción del documento de Política de Seguridad de la Información se tomó en cuenta la Norma Técnica Peruana NTP-ISO/IEC 27002:2005 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información; la cual ha sido aprobada mediante Resolución Ministerial Nº 246-2007-PCM y la que actualmente sigue en vigencia. No se tomó como referencia la ISO/IEC 27002: 2013 ya que aún esta norma no ha sido aprobada en nuestro país, además no existe un proyecto de norma para su futura publicación. Por ese motivo este documento tomara como base la NTP-ISO/IEC 27002:2005.

Así mismo para validar las Políticas del SGSI se debe alinear con lo que exige la NTP ISO/IEC 27001: 2014 en el numeral 5.2 Política; en la que establece los requisitos para su definición:

"*La alta dirección debe establecer una política de seguridad de la información que:*

a) Es apropiada al propósito de la organización;

b) Incluye objetivos de seguridad de la información o proporcione un el marco de referencia para fijar los objetivos de seguridad de la información;

c) Incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información;

d) Incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información

La política de seguridad de Información debe

e) Estar disponible como información documentada;

f) Estar comunicada dentro de la organización; y

g) *Estar disponible para las partes interesadas, según sea apropiado*" (NTP-ISO/IEC 27001, 2014)

A partir de esto se puede indicar lo siguiente sobre la política de seguridad de información desarrollada:

1. Es adecuada al propósito del CGT, y la forma como ha sido redactada de acuerdo a su contexto. Para ello se tomó en cuenta el contexto de todo el CGT, el contexto de la Oficina de TI, la falta de inversión así como las funciones que desempeñan los

trabajadores o colaboradores de la institución y de la misma Oficina de TI, con ello se ajustaron los diferentes controles que se listan en esta política.

2. Los objetivos de seguridad de la Información se incluyen en el Documento de Políticas de SI.
3. El compromiso de cumplimiento está redactado como parte de la política.
4. Así mismo la Política de SI está debidamente documentada y analizada por las áreas correspondientes, y ha sido aprobada por la dirección del CGT. Solo faltaría ser comunicada de manera formal y estar a disposición de todo el personal.

3.2.3. Análisis de la Organización

El análisis de la situación actual en el CGT es importante, por cuanto hay requerimientos existentes y activos de información que deberían ser considerados cuando se implementen el SGSI. Las actividades descritas en esta fase pueden ser emprendidas en paralelo con aquellas descritas en “Alcances y Políticas de SI” por razones de eficiencia y practicidad.

La información recopilada a través del análisis de la seguridad de la información debería:

a. Proveer a la Dirección de un punto de inicio (es decir, datos básicos correctos)
b. Identificar y documentar las condiciones para la implementación
c. Proveer entendimiento claro y bien establecido de las instalaciones de la organización
d. Considerar las circunstancias particulares y la situación de la organización
e. Identificar el nivel de protección deseado de la información
f. Determinar la compilación de la información requerida para toda o parte de una empresa dentro del alcance de implementación propuesto.

Es por ello que se definirán los requerimientos de seguridad de la información y se identificara activos que están dentro del alcance del SGSI, la cual incluirá información como descripción de los principales procesos del CGT, identificación de activos de información de los principales procesos de la organización, etc.

A partir de ello se genera una evaluación de seguridad de la información el cual nos muestra el estado actual de seguridad de la información de la organización y su evaluación incluyendo controles de seguridad existentes y deficiencias de la organización identificadas.

3.2.4. Evaluación del riesgo y selección de las opciones de tratamiento de riesgo.

a) Definir proceso de evaluación de riesgo de la seguridad de la información.

Definir la metodología de evaluación del riesgo nos permitirá identificar, analizar y evaluar los riesgos de la seguridad de la información, para luego seleccionar las opciones de tratamiento del riesgo, los objetivos de control y los controles más adecuados.

La metodología utilizada en la presente investigación para la evaluación de riesgo está basada en la Norma Técnica Peruana ISO/IEC 27005:2009 en la que se establece lineamientos para la gestión del riesgo en seguridad de la información, orientados a la administración de los riesgos que podrían comprometer la seguridad de la información del CGT.

Esta metodología se apoya en los conceptos generales especificados en la norma Técnica Peruana ISO/IEC 27001 y está diseñado para asistir a la implementación satisfactoria de la seguridad de la información en base a un enfoque de gestión del riesgo.

b) Estructura del procedimiento

Esta metodología contiene la descripción del proceso de gestión del riesgo en seguridad de la información y sus actividades; y se tratarán los siguientes temas:

a) Bases.
b) Vista panorámica del proceso de gestión del riesgo en seguridad de la información.
c) Establecimiento del contexto.
d) Evaluación del riesgo.
e) Tratamiento del riesgo.
f) Aceptación del riesgo.
g) Comunicación del riesgo.
h) Monitoreo y revisión del riesgo.

c) Alcance y límites del proceso de gestión del riesgo en SI

El alcance del proceso de gestión del riesgo en seguridad de la información debe definirse para asegurar que se tomen en cuenta todos los activos relevantes en la evaluación del riesgo. Para ello previamente se identificó los límites del SGSI para enfrentar los riesgos que puedan surgir dentro de esos límites.

Luego se hizo un análisis de la información antes recolectada sobre el CGT para seleccionar aquella que tiene relevancia con el proceso de gestión del riesgo en seguridad de la información.

La estructura de esta sección de la investigación se hizo en base al "Anexo A – Definición del alcance y límites del proceso de Gestión de riesgo en seguridad de la Información de la NTP ISO/IEC 27005". La estructura de este capítulo es la siguiente:

- Consideraciones generales: Se muestra las características generales del CGT, como su misión, visión, análisis FODA, organigrama entre otros.
- Alcance del Sistema de gestión de Seguridad de la Información: Se muestra el alcance ya establecido anteriormente para el SGSI.
- Lista de restricciones que afectan la organización: En esta sección se mostrará las restricciones que afectan al CGT y determinan su orientación en seguridad de la información. Su fuente puede estar dentro de la institución, en cuyo caso tiene cierto control sobre ella o fuera del CGT y, por lo tanto, generalmente no es controlable.
- Lista de las referencias legislativas y regulatorias aplicables a la organización: Se identificaron los requisitos regulatorios que se aplican en el CGT como leyes, decretos, regulaciones internas y externas, etc.
- Lista de restricciones que afectan el alcance: Se han identificado las restricciones que tienen un impacto en el alcance, estas se añaden a las restricciones que afectan la organización que se han determinado anteriormente y posiblemente las cambian. Se muestran restricciones técnicas y temporales.
- Criterios básicos para el enfoque de Gestión de Riesgo: se expuso un enfoque de gestión de riesgo en la cual resuelva los criterios básicos como: criterios de evaluación del riesgo, criterios de impacto, criterios de aceptación del riesgo. Además, se debe evaluar si el CGT dispone de los recursos necesarios para:
    - Una evaluación del riesgo y establecer un plan de tratamiento del riesgo.
    - Definir e implementar políticas y procedimientos, incluyendo la implementación de controles seleccionados.
    - Monitorear controles.
    - Monitorear el proceso de gestión del riesgo en seguridad de la información.

d) Identificación, valorización de activos y evaluación de impacto

En este capítulo se listan los activos que están dentro del alcance del SGSI, los cuales fueron identificados realizando una serie de

entrevistas a las áreas que forman parte del alcance y luego se clasificaron de acuerdo a los tipos de activos que muestra la norma NTP ISO/IEC 27005:2008. Esta norma distingue dos tipos de activo:

- Los activos primarios:
  - Procesos y actividades del negocio
  - Información
- Los activos de apoyo (sobre los cuales descansan los activos primarios):
  - Hardware
  - Software
  - Red y comunicaciones
  - Personal
  - Sitio
  - Estructura de la organización

El siguiente paso luego de la identificación del activo es valorizar los activos. Esta tarea se inicia con acordar la escala que se debe utilizar y los criterios para asignar una ubicación particular en esa escala por cada activo en base a la valorización.

a. Criterios.

El criterio elegido para la valorización de activos son los costos incurridos debido a la pérdida de confidencialidad, integridad y disponibilidad como resultado de un incidente.

- **Confidencialidad**: Indica que la información del activo no puede ser vista por personal no autorizado.
- **Integridad**: El activo debe estar correcto y completo y debe ser protegido por cambios no autorizados, no previstos o accidentales.
- **Disponibilidad**: El activo debe estar disponible y utilizable en el momento que se necesite.

b. Escala

En este caso se valorará una escala cuantitativa de acuerdo a los criterios de disponibilidad, integridad y confidencialidad, siendo el número 1 el de menor relevancia y el número 3 con el valor más relevante. En la siguiente tabla se muestra los criterios y sus respectivos valores.

Tabla N° 29. Criterios para valorización de activos

Criterio	Valor en escala	Descripción
Disponibilidad	1	El activo debe estar disponible por lo menos 25% del tiempo que se necesite. No existe riesgo operacional, reputacional, ni legal si el activo de información se ha eliminado o no está disponible.
	2	El activo debe estar disponible por lo menos 50% del tiempo que se necesite. Si no lo estuviera o si fuese destruido puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe estar disponible el 100% del tiempo que se necesite. Si no lo estuviera o si fuese destruido ocasionará daños graves o hasta catastróficos para la organización, afectarán los intereses legales, operacionales o reputacionales, y causarán pérdidas financieras.
Integridad	1	El activo debe estar correcto y completo por lo menos el 25% de las veces que se necesite. No existe pérdidas financieras ni riesgo operacional, reputacional, ni legal.
	2	El activo debe ser correcto y completo al menos el 50% de las veces que se necesita. Puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe ser correcto y completo el 100% de las veces utilizadas. De no cumplir con lo anterior, puede causar daños graves o hasta catastróficos para la organización, y afectará los intereses legales, operacionales o reputacionales, además de pérdidas financieras significativas.
Confidencialidad	1	El activo es publicada o de conocimiento del público en general, por lo tanto, no existe ningún riesgo legal, reputacional, operacional, ni financiero.
	2	El activo podrá ser divulgado hacia los colaboradores. Si se cumple con lo anterior no será perjudicial para los intereses legales, reputacional, operacional, ni financiero.
	3	El activo contiene información altamente sensible. Su divulgación puede causar daños graves o hasta catastróficos, afectando los intereses legales, reputacionales, y financieros.

Fuente: Desarrollo Propio

Como resultado de la identificación de activos se obtiene un listado de los activos involucrados en el alcance del SGSI relacionados con su respectivo propietario y con su valorización. El valor final del activo (Valor de Criticidad) será el promedio de los tres valores en base a los criterios (disponibilidad, integridad y confidencialidad).

En la Tabla siguiente se describe el valor cualitativo promedio del activo (Valor de Criticidad):

Tabla N° 30. Valor de Criticidad del activo

Valor promedio de activo	Descripción
3 – ALTO	Alto, contiene información confidencial y en muchos casos la disponibilidad debe ser del 100%.
2 – MEDIO	Medio, no contiene información sensible, pero debe cumplir con algunos criterios como disponibilidad e integridad.
1 – BAJO	Bajo, los activos ubicados en este valor promedio, son activos de carácter público.

Fuente: Desarrollo Propio

En la siguiente tabla se muestra el resultado de la evaluación de los activos seleccionados de acuerdo con los criterios antes mencionados, un resumen de esta tabla es la siguiente:

Tabla N° 31. Modelo de inventario y valorización de activos

	PROPIETARIO DEL ACTIVO	C	I	D	PROMEDIO	VALOR DE CRITICIDAD
ACTIVOS PRIMARIOS						
Gestión Administrativa	Oficina General de Administración	3	3	3	3	ALTO
Gestión tributaria	División de recaudación y control de deuda	2	3	3	3	ALTO
Programa de apoyo social	Gerencia de desarrollo económico y social	2	2	2	2	MEDIO
Servicios públicos	División de servicios al administrado	2	2	2	2	MEDIO
Control Interno.	Oficina de Control Interno	3	3	1	2	MEDIO

Fuente: Desarrollo Propio

Una vez realizada la valorización de activos se identifican las amenazas. Para este paso se utilizó la lista de amenazas que muestra la metodología MagerIT y se seleccionaron aquellas que podrían materializarse en el CGT, luego en una matriz se hizo una relación entre amenazas posibles y los activos identificados. Este cuadro tendrá el siguiente formato:

Tabla N° 32. Modelo de listado de amenazas posibles VS activos identificados

Amenazas	Activos Primarios		Activos de Apoyo					
	Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
[N] Desastres naturales								
[N.1] Fuego	√	√	√		√		√	
[N.2] Daños por agua	√	√	√		√		√	
[N.*] Desastres naturales	√	√	√		√		√	

Fuente: Desarrollo Propio

Luego se identificaron en una tabla las vulnerabilidades agrupadas por tipo de activo, y finalmente se realizó una evaluación del impacto. Dicha evaluación del impacto tendrá la siguiente estructura por cada amenaza antes identificada:

Tabla N° 33. Evaluación de la amenaza

[código] descripción sucinta de la amenaza que puede pasar	
Tipos de activos que se pueden ver afectados por este tipo de amenazas	Impacto generado producto de la amenaza materializada, ordenados de más a menos relevante
Vulnerabilidad que la amenaza utiliza para que pueda materializarse.	

Fuente: Desarrollo Propio

c. Análisis y evaluación del riesgo en SI

Este tipo de evaluación está dirigido a una visión más global de la organización y de sus sistemas de información, considerando los aspectos de la tecnología como independientes de las cuestiones empresariales. Al hacer esto, el análisis del contexto se concentra en el negocio y el entorno operático que en los elementos tecnológicos. (NTP-ISO/IEC 27005, 2009)

En otras palabras la evaluación del riesgo de alto nivel considera los valores empresariales de los activos de información y los riesgos desde el punto de vista del negocio de la organización.

Se comenzó por este tipo de evaluación ya que como es la primera vez que realizan una evaluación de riesgo al CGT, esta

presenta un enfoque simple inicial y con ello el programa de evaluación de riesgo gane más aceptación.

Mencionar también que los riesgos que se presentan en una evaluación del riesgo de alto nivel frecuentemente son dominios de riesgo más generales que los riesgos específicos identificados. Por ello se formuló un inventario de riesgo con este tipo de evaluación tomando en cuenta los doce dominios seleccionados en el alcance de la norma NTP ISO/IEC 27001:2014, los cuales siguen el siguiente formato por cada dominio:

Tabla N° 34. Inventario de riesgos en SI de alto nivel

DOMINIO	RIESGO	DENOMINACION
Dominio 1		A.5 Política de seguridad
	R1	A.5.1 Riesgo asociado a la Dirección de la Gerencia para la seguridad de la información.
		Inconvenientes presentados por la falta de proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos de la organización, las leyes y regulaciones relevantes.

Fuente: Desarrollo Propio

Después de realizar un inventario de riesgo, se desarrolló un matriz en donde se relacionan los riesgos identificados anteriormente con los activos primarios y de apoyo del CGT. Este cuadro tendrá el siguiente modelo:

Tabla N° 35. Matriz de riesgos vs activos

MATRIZ DE RIESGOS VS ACTIVOS										
RIESGOS			Activos primarios		Activos de apoyo					
			Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
Dominio 1		A.5 Política de seguridad								
	R1	A.5.1 Riesgo asociado a la Dirección de la Gerencia para la seguridad de la información.						√		√

Fuente: Desarrollo Propio

Posteriormente la siguiente tabla muestran la evaluación cualitativa del riesgo en base a la probabilidad e impacto teniendo en cuenta una escala de 5X5, donde 1: poco impacto o poca probabilidad y 5: gran impacto o probabilidad.

Se evaluará la probabilidad de ocurrencia y grado de impacto de los riesgos definidos de manera general con criterios de evaluación. Este cuadro tendrá el siguiente formato:

Tabla N° 36. Matriz general de riesgo de alto nivel

MATRIZ GENERAL DE RIESGOS PROBABILIDAD E IMPACTO													
RIESGO			PROBABILIDAD						IMPACTO				
			1	2	3	4	5		1	2	3	4	5
Dominio 1		A.5 Política de seguridad											
	R1	A.5.1 Riesgo asociado a la Dirección de la Gerencia para la seguridad de la información.			X						X		

Fuente: Desarrollo Propio

Luego se colocara cada riesgo de acuerdo con las valorizaciones que se dio en el mapa de riesgo general. Según este mapa de riesgo se puede concluir que de las matrices desarrolladas, los riesgos afectan de manera similar tanto a los activos primarios

como de apoyo, por lo que al ocurrir un evento no deseado sobre alguno de ellos, se alterará su funcionamiento normal de manera similar para todos los procesos.

Otras de las consideraciones que se puede desprender de las matrices, es que la mayoría de los riesgos se ubican en la zona de tolerancia aceptable y zona de tolerancia alta, son tres riesgos los que se ubican en la zona de tolerancia extrema, lo que indica que se viene haciendo los esfuerzos necesarios para tratar de aceptar el riesgo mediante la implementación de controles, aunque estos no estén implementados de la manera adecuada.

Criterio de aceptación: Del análisis del mapa de riesgo anterior se puede concluir que se han registrado 10 riesgos en la Zona de Tolerancia Aceptable en donde se puede apreciar que algunos controles han minimizado el impacto de los riesgos, pero no se debe dejar de evaluarlos. Además se han registrado 04 riesgos en la Zona Tolerancia Moderada y 14 riesgos en la Zona Tolerancia Alta donde se aceptan los riesgos y el CGT trata de controlarlos.

Así mismo, se han registrado 03 riesgos en la Zona Extrema, estos deberían ser evaluados, sin embargo para un mayor estudio de estos es necesario realizar una evaluación detallada del riesgo para su posterior tratamiento.

Es por ello que se pasara a realizar el segundo tipo de evaluación y también para poder identificar los riesgos potenciales ya que con una evaluación de riesgo de alto nivel no se podría realizar.

Evaluación detallada del riesgo en seguridad de la información

El proceso de evaluación detallada del riesgo en seguridad de la información incluye una identificación y valorización profunda de los activos, la evaluación de amenazas a esos activos y la evaluación de vulnerabilidades. Los resultados de esas actividades se utilizan entonces para evaluar los riesgos y luego identificar el tratamiento del riesgo.

Para el inventario de riesgos en seguridad de la información de la evaluación detallada se agruparon los riesgos en dos tipos tomando en cuenta los activos primarios y de apoyo para una mejor comprensión, de acuerdo al siguiente cuadro:

Tabla N° 37. Denominación del riesgo según el tipo de activo

Código del Riesgo	Denominación
RP	Riesgos que afectan a los activos primarios del CGT.
RA	Riesgos que afectan a los activos de apoyo del CGT.

Fuente: Desarrollo Propio

A partir del cuadro anterior se identificaron los siguientes riesgos, luego se evaluó la probabilidad de ocurrencia y su grado de impacto. Finalmente, se coloca cada riesgo de acuerdo con las valorizaciones que se dio en el mapa de riesgo general.

Con todo ello, se puede concluir que del análisis del mapa de riesgo general anterior se han registrado 02 riesgos en la Zona de Tolerancia Aceptable, 11 riesgos en la Zona Tolerancia Moderada y 79 riesgos en la Zona Tolerancia Alta donde los riesgos se encuentran controlados de alguna manera pero debe continuarse su evaluación periódica. Así mismo se han registrado 24 riesgos en la Zona Extrema, los cuales deben ser tratados para poder reducirlos.

e) Identificación y evaluación de las opciones para el tratamiento del riesgo en SI.

Con la lista de riesgos priorizada de acuerdo con criterios de evaluación del riesgo en relación con los escenarios de incidentes que llevan a esos riesgos se debe seleccionar controles para reducir, retener, evitar o transferir los riesgos y un plan del tratamiento del riesgo definido.

La Gerencia cuenta con cuatro opciones para el tratamiento del riesgo que no se excluyen mutuamente. A veces el CGT puede beneficiarse sustancialmente por una combinación de opciones como la reducción de la posibilidad de riesgos, la reducción de sus consecuencias, y la transferencia o retención de cualquier riesgo residual.

El objetivo de esta parte es la definición de un plan de tratamiento del riesgo que identifique claramente la prioridad ordenando, cuáles tratamientos del riesgo individual debe implementarse. Para esta tarea previamente se definieron las opciones de tratamiento (Reducción del riesgo, Retención del riesgo, evitamiento del riesgo y transferencia del riesgo), posteriormente se hizo una selección de los objetivos de control y controles para el tratamiento del riesgo y con ello se puede definir el plan de tratamiento. En este plan se mostraran

los riesgos extremos, con la decisión de aceptación (Estrategia), así como el propietario de dicho riesgo, teniendo como fin responsabilizarlo por monitorear el riesgo identificado y gestionar el plan de tratamiento, independiente de que él sea el responsable de implementar las acciones registradas en dicho plan.

Así mismo la presente tesis no determinara los riesgos residuales. Sin embargo, se propone que la Oficina de TI haga la evaluación del plan de tratamiento para ver los controles planteados y con ellos obtener el riesgo residual, para luego realizar una actualización o reiteración de la evaluación del riesgo, tomando en cuenta los efectos esperados del tratamiento propuesto del riesgo. Además si el riesgo residual todavía no cumple con los criterios de aceptación del riesgo del CGT, puede ser necesaria una nueva iteración del tratamiento del riesgo antes de proceder a la aceptación del riesgo.

f) Aceptación del riesgo en SI

Es importante que la Gerencia revise y apruebe el plan de tratamiento del riesgo propuesto, así mismo tienen la responsabilidad de la decisión de aceptar los riesgos residuales, una vez implementados los controles.

Sin embargo en algunos casos el nivel de riesgo residual puede no cumplir con los criterios de aceptación del riesgo porque los criterios que se están aplicando no toman en cuenta algunas circunstancias prevalecientes y por lo tanto se tendría que aceptar algún riesgo debido a que el costo de reducción de dicho riesgo es demasiado alto. Es por ello que quienes toman las decisiones pueden tener que aceptar los riesgos que no satisfacen los criterios de aceptación normal. Si esto es necesario, quien toma las decisiones debería comentar explícitamente los riesgos e incluir una justificación para que la decisión pueda pasar por encima de los criterios normales de aceptación del riesgo.

g) Comunicación del riesgo en SI

La comunicación del riesgo es una actividad para lograr acuerdos sobre cómo manejar los riesgos intercambiando y/o compartiendo información sobre el riesgo entre quienes toman las decisiones y otros interesados. La información incluye, pero no se limita a la existencia, naturaleza, forma, posibilidad, gravedad, tratamiento y aceptabilidad de los riesgos.

La comunicación es bi-direccional ya que involucra un dialogo en ambas direcciones entre los interesados. Esto es importante ya que se puede tener un impacto significativo en las decisiones que se deben tomar. La comunicación asegurará que los responsables de

implementar la gestión del riesgo y aquellos que tienen intereses particulares comprendan la base sobre la cual se toman las decisiones y las acciones particulares que se requieren.

El riesgo para operaciones normales, así como las situaciones de emergencia serán comunicados haciendo uso de los formatos establecidos lo que permitirá que el Comité de Seguridad de la Información y la Gerencia debatan los riesgos, su priorización y su tratamiento apropiado y aceptación.

Es importante cooperar con el Comité de Seguridad de la Información para coordinar todas las tareas relacionadas con la comunicación del riesgo. Esto es crucial en el caso de acciones de comunicación de la crisis.

Como resultado de la comunicación del riesgo se tendrá un plan de comunicación desarrollado y aprobado por el Comité de Seguridad de la información, además será el Oficial de Seguridad de la información quien velara por el cumplimiento de la comunicación en el CGT.

h) Preparar enunciado de aplicabilidad (SOA)

Este documento, requerido por la Norma Técnica Peruana ISO/IEC 27001:2014, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados.

En este documento se ha registrado todo lo que se ha realizado y se va a realizar en el futuro inmediato para que la seguridad de la información del CGT llegue al nivel que se haya estimado apropiado para sus necesidades y recursos.

Razón por la cual la declaración de aplicabilidad debe incluir los controles apropiados en el punto anterior.

Para cada uno de los controles debe reflejarse en este documento:

- Si está implantado actualmente en la organización, con una breve descripción de por qué se aplica.
- Si se va a implantar, es decir, si es uno de los controles escogidos para mitigar el riesgo, junto con las razones para haberlo seleccionado.
- Si no se va a implantar, y entonces hay que exponer los motivos que han llevado a esta decisión.

El principal objetivo de este documento es que, al tener que repasar todos y cada uno de los controles, se hace una comprobación de que no se ha pasado por alto ningún control por error o descuido, que podría ser útil o necesario para la gestión de la seguridad de la información.

Este documento es un registro de los resultados finales del SGSI, ya que concreta de manera clara y directa en qué consiste el sistema gestión de seguridad de la información.

Se utilizará un código de colores que indica el estado en que se encuentra el control para una mejor gestión de su estado (verde: control implantado, amarillo: control en proceso de implantación, rojo: necesario pero no se ha iniciado su implantación, y sin color: control que no es necesario por el momento y no se ha iniciado su implantación).

3.2.5. Verificación del SGSI

Esta fase pretende verificar si el desarrollo del plan de implementación del Sistema de Gestión de Seguridad de la Información propuesto considera los puntos descritos en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Tabla N° 38. Relación de requisitos de la NTP-ISO/IEC 27001:2014 con el documento del SGSI del CGT

Requerimientos Obligatorio para el SGSI				¿Cumple?	Documentos del SGSI del CGT
4			**CONTEXTO DE LA ORGANIZACIÓN**		
	4.1		Comprender la organización y su contexto	**SI**	**Documento Alcance del SGSI:** 3.1. Características claves de la organización (su función, estructura, servicios, etc.) del documento sobre el alcance del SGSI
			La organización debe determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI		
	4.2		Comprender las necesidades y expectativas de las partes interesadas	**SI**	**Documento Alcance del SGSI:** 3.6. Identificación de las partes interesadas
			La organización debe determinar las partes interesadas y los requisitos de estas partes interesadas relevantes a la seguridad de la información		
	4.3		Determinar el alcance del sistema de gestión de seguridad de la información	**SI**	**Documento Alcance del SGSI:** 3.3. Los procesos organizacionales en el alcance
			La organización debe determinar los límites y la aplicabilidad del sistema de gestión de Seguridad de la información para establecer su alcance.		
	4.4		Sistema de gestión de seguridad de la información	**SI**	**Documento del SGSI**
			La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, en conformidad con los requisitos de esta Norma Técnica Peruana.		
5			**LIDERAZGO**		

	5.1		Liderazgo y compromiso	SI	**Documento de la Política General de Seguridad de la Información** 7.3. Responsabilidad
			La alta dirección debe demostrar liderazgo y compromiso respecto del sistema de gestión de seguridad de la información		
	5.2		Política	SI	**Documento de la Política General de Seguridad de la Información** 2. Objetivos
			La alta dirección debe establecer una política de seguridad de la información que sea apropiada al propósito de la organización		
	5.3		Roles, responsabilidades y autoridades organizacionales	SI	**Documento de la Política General de Seguridad de la Información** 8. Aspectos organizativos de la seguridad de la información
			La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.		
6			**PLANIFICACION**		
	6.1		Acciones para tratar los riesgos y las oportunidades		
		6.1.1	Generalidades	SI	**Documento de Sistema de Gestión de Seguridad de la Información** 1.4 Definición del alcance y límites de proceso de Gestión del riesgo en Seguridad de la Información
			Cuando se planifica para el sistema de gestión de seguridad de la información, la organización debe considerar los asuntos referidos en el numeral 4.1 y los requisitos referidos en el numeral 4.2 y determinar los riesgos y oportunidades que necesitan ser tratados		
		6.1.2	Valoración del riesgo de seguridad de la información	SI	**Documento de Sistema de Gestión de Seguridad de la Información** 1.3.5 Evaluación del riesgo en Seguridad de la Información – 1.5 Identificación y valorización de activos y evaluación de impacto – 1.6. Análisis y evaluación de riesgo en seguridad de la información
			La organización debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información		
		6.1.3	Tratamiento de riesgos de seguridad de la información.	SI	**Documento de Sistema de Gestión de Seguridad de la Información** 1.3.6. Tratamiento del riesgo en seguridad de la información – 1.7. Identificación y evaluación de las opciones para el tratamiento del riesgo en seguridad de la información
			La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información		
	6.2		Objetivos de seguridad de la información y planificación para conseguirlos	SI	**Documento de Sistema de Gestión de Seguridad de la Información** 1.7.3. Plan de tratamiento
			La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.		

Fuente: Desarrollo Propio

IV. RESULTADOS Y DISCUSIÓN

4.1. Establecimiento y manejo del sistema de gestión de seguridad de la información

4.1.1. Alcance y límites del SGSI

Este Sistema de Gestión de Seguridad de la Información cubre doce dominios de la norma NTP-ISO/IEC 27001:2014 con la finalidad de salvaguardar la información, sistemas de información, procesos y personas del CGT, siendo estos:

1. **Política de seguridad de la Información:** Es donde se estipulan las políticas con respecto a la seguridad de la Información para el CGT.
2. **Organización de la seguridad de la información:** Busca administrar la seguridad dentro del CGT (Roles, compromisos, autorizaciones, etc.).
3. **Seguridad en Recursos Humanos:** Dominio orientado a asegurar que todo el personal del CGT (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales u otros) entiendan sus responsabilidades y sean adecuados para los roles a desempeñar minimizando los riesgos relacionados con el recurso humano.
4. **Gestión de activos:** Referido al mantenimiento y protecciones apropiadas de todos los activos de información.
5. **Control de accesos:** Busca controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.
6. **Seguridad física y ambiental:** Destinado a prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones del CGT y a su información.
7. **Seguridad de las operaciones:** Para asegurar operaciones correctas y seguras en el procesamiento de información.
8. **Seguridad en las comunicaciones:** Busca asegurar la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.
9. **Adquisición, desarrollo y mantenimiento de sistemas de información:** Básicamente busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.
10. **Gestión de incidentes en la seguridad de información:** Permitir que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicadas de tal manera que se tome una acción correctiva adecuada en el momento indicado.
11. **Aspectos de seguridad de información en la gestión de continuidad del negocio:** Dominio enfocado en reaccionar en contra de interrupciones a las actividades del CGT y en proteger procesos críticos de los efectos de fallas mayores en los sistemas de información o desastres, y asegurar que se resuelvan a tiempo.
12. **Cumplimiento:** Destinado a prevenir el incumplimiento total o parcial de cualquier ley, norma, regulación u obligación contractual de los requerimientos de seguridad.

Se excluyó el dominio de “A.10. Criptografía”, ya que actualmente el CGT cuenta con sus propios controles para proteger y no divulgar la información confidencial que maneja (uso de claves y contraseñas); es por ello que por el momento no es necesario utilizar controles criptográficos en la información confidencial, debido a que implementar este tipo de controles sería muy complejo puesto que se tendría que hacer uso de algoritmos de encriptación, hacer uso de un modelo de criptografía (simétrica o asimétrica) y contar con claves al cifrar cierta información, aunque más adelante sería lo más apropiado implementarlos.

Además se excluyó el dominio de “A.15. Relación con los proveedores”, ya que solo se hizo un estudio de la gestión interna del CGT; sin embargo, más adelante se tendría que asegurar la protección de los activos de la organización que sean accesibles a los proveedores implementando este tipo de dominio.

Del mismo modo el Sistema de Gestión de la Seguridad de la Información (SGSI), es de aplicación a todo el CGT, sin embargo se enfocaran en las áreas cuyos procesos son más críticos.

A fin de identificar los procesos críticos del CGT se realizó un proceso para justificar la elección de las direcciones y gerencias con mayor importancia en el CGT las cuales formaran parte del alcance del SGSI. Este proceso de elección puede ser visualizado en el ítem “Los procesos organizacionales en el alcance” del Documento Alcance del SGSI del CGT y en base a estas direcciones y/o gerencias seleccionadas podemos determinar los procesos críticos.

Según el proceso de elección antes mencionado, las áreas que serán incluidas dentro del alcance del SGSI por su interacción con el sistema y el nivel de criticidad de los procesos que se desarrollan dentro de ellas son:

a. **Oficina de Control Interno**
b. **Órganos de apoyo**
   - Oficina general de Administración, con sus unidades de Contabilidad y Finanzas, Tesorería, RRHH, Abastecimiento y Control Patrimonial.
   - Oficina de Tecnología de la Información.
c. **Gerencia de Operaciones**
   - División de recaudación y control de deuda
   - División de servicios al administrado

Se tomó en cuenta la **Oficina de Control Interno** ya que es la encargada de realizar una auditoria interna al CGT, cautelando que los hallazgos, observaciones, conclusiones y recomendaciones de estas auditorías sean válidas, apropiadas y pertinentes, dentro de un sistema de calidad que busca la eficacia y eficiencia de las actividades que realicen las Gerencias y Direcciones de la institución, de acuerdo a las Normas Técnicas de Control, dictadas por la Contraloría General de la República. Es por ello que se tomara en cuenta por su importancia e influencia en el CGT y también porque tienen cierta responsabilidad en el Sistema de Gestión de Seguridad de la Información.

También se tomó en cuenta la **Oficina General de Administración** la cual se encarga de organizar, dirigir y controlar la gestión de los recursos económicos y financiero del CGT, en función de las necesidades de ejecución del Presupuesto y así mismo se incluyó a todas sus unidades: con sus unidades de Contabilidad y Finanzas, Tesorería, RRHH, Abastecimiento y Control Patrimonial.

Del mismo modo forma parte del alcance, la **Gerencia de Operaciones** ya que son la esencia del CGT, debido a que una de los principales compromisos que incluso están inmerso en la misión del CGT es la responsabilidad social y el desarrollo económico con la población Chiclayana y la prestación de servicios públicos en todos los niveles.

Es por ello que solo se tomaran estas áreas para el alcance del SGSI sin embargo posteriormente y como parte de la mejora continua exigida por la metodología PDCA aplicable a dichos sistemas, se puede ir incorporando al resto de áreas.

4.1.2. Política del Sistema de Gestión de Seguridad de la Información.

a. Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el CGT y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del CGT.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de la alta Gerencia CGT y de las áreas y/o unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

b. Objetivo

- Proteger los recursos de información del CGT y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Mantener la Política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

c. Responsabilidad

Todos los Gerentes, Jefes de Áreas y Unidades Organizativas y personal operativo y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del CGT, cualquiera sea su situación en la misma, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

- Oficial de Seguridad de la Información. cumplirá funciones de monitoreo y seguimiento relativas a la seguridad de los sistemas de información del CGT, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.
- Propietario de información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
- La Oficina General de Administración o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información. Asimismo, tendrá a su cargo la suscripción de los Acuerdos de Confidencialidad.
- Oficina de Tecnologías de la Información cumplirá la función de cubrir los requerimientos de seguridad establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del CGT. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.
- Usuario de la Información son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.
- Control Interno es responsable de solicitar se practiquen auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información al área de Tecnologías de la Información y Procesos.

d. Base legal

- Resolución Ministerial Nº 246-2007-PCM, que aprueba la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.
- Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del sistema nacional de informática.

e. Cumplimiento obligatorio

El cumplimiento de las políticas y estándares definidos en el presente documento de Información es obligatorio y debe ser considerado como una condición en los contratos del personal.

Toda excepción a las políticas debe ser documentada y aprobada por la Oficina de TI, detallando el motivo que justifica el no cumplimiento de las políticas establecidas en el presente plan.

4.2. Análisis de la organización

El análisis de la problemática del CGT en relación a la seguridad de la información y la gestión de TI fue desarrollado como parte de la descripción del problema de la investigación.

4.3. Declaración de aceptación, compromiso y cumplimiento del SGSI

El CGT, muestra una responsabilidad social con la población generando el mejoramiento en la calidad de vida por cuanto están dispuestos a la prestación de servicios públicos en todos los niveles, mediante la ejecución de obras de corto y largo plazo que garantizan ser oportunos y óptimos con una administración transparente, capacidad de gestión adecuada y política concertadora, abierta al diálogo y al cambio social.

Dentro de este contexto el CGT adoptará, aceptará, aprobará, cumplirá, revisará y actualizará el plan de gestión en seguridad de información el mismo que será acorde con los lineamientos y objetivos de la entidad, en los siguientes aspectos de la seguridad de la información:

- **Disponibilidad**: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- **Confidencialidad**: La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados.
- **Integridad**: La propiedad de salvaguardar la exactitud e integridad de los activos.

Dicho plan se encuentra basado en un enfoque de riesgo operativo; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información con la finalidad de buscar mantener la confidencialidad, integridad y disponibilidad sobre los activos de información propiedad del CGT.

El CGT declara:

1. El compromiso por parte de todos los niveles de la entidad en adoptar, aceptar, aprobar, cumplir, revisar y actualizar las políticas, lineamientos y controles que forman parte del Sistema de gestión de Seguridad de Información.
2. El compromiso de identificar claramente en el ámbito de la seguridad los roles, responsabilidades y sanciones por incumplimiento por parte del personal y terceros.
3. El compromiso de conformar el Comité de gestión de seguridad de información el mismo que mantendrá una participación activa de acuerdo a sus roles y responsabilidades.
4. El compromiso de adoptar, aceptar, aprobar, ejecutar y revisar periódicamente una o varias metodologías formales de análisis

y evaluación de riesgos. La metodología permitirá identificar el nivel de riesgo que afecta los activos de información, procesos, subprocesos y elementos de apoyo de propiedad del CGT.

5. El compromiso en implantar, monitorear y gestionar el riesgo operativo y de información mediante los controles administrativos y tecnológicos que el CGT crea conveniente implantar con la finalidad de mitigar o reducir el impacto ante un evento que pretenda vulnerar la seguridad de la información. Dando por aprobados los riesgos residuales presentados en este documento.
6. El compromiso de elaborar, mantener y ejecutar periódicamente programas de capacitación, concientización y entrenamiento en temas de seguridad de información dirigido al personal y terceros.
7. El compromiso de auditar periódicamente el cumplimiento del plan de gestión de seguridad de información por parte del CGT.
8. Entender que es necesario mantener un compromiso diario con las actividades relacionadas con la seguridad de información.

Por lo expuesto:

El CGT en todos sus niveles de Organización declara su firme compromiso en adoptar, aceptar, aprobar, cumplir, monitorear, revisar y actualizar el plan de gestión de seguridad de información en conformidad al marco de referencia NTP ISO/IEC 27001:2014.

4.4. Evaluación de los riesgos de TI

La metodología aplicada para la valuación de riesgo está basada en la Norma Técnica Peruana ISO/IEC 27005:2009 en la que se establece lineamientos para la gestión del riesgo en seguridad de la información, orientados a la administración de los riesgos que podrían comprometer la seguridad de la información del CGT.

4.4.1. Identificación, valorización de activos

a. Identificación de activos

Para realizar una valorización de activos, el CGT ha identificado sus activos dentro del alcance, de estos se puede distinguir dos tipos de activo:

- Los activos primarios: son los procesos e información centrales del CGT, lo que es más apropiado para diseñar una política de seguridad de la información o un plan de continuidad del negocio.
    - Procesos y actividades del negocio
        - Gestión Administrativa.
        - Gestión operativa
        - Programa de apoyo social
        - Servicios públicos
        - Control Interno.

- Información

  Toda la información gubernamental es pública y los particulares tendrán acceso a la misma en los términos que la propia ley señala esto según Ley N° 27806 que en su artículo 3 en la que se señala: “Toda información que posea el Estado se presume pública, salvo las excepciones expresamente previstas por el Artículo 15 de la presente Ley”.

  - Información contenida en las bases de datos pertenecientes al CGT.
  - Información contenida en sistemas gubernamentales externos: SIGA y SIAF.
  - Información contenida en el Portal Web Institucional.
  - Información confidencial:
    - Información protegida por el secreto tributario y tecnológico que están regulados, unos por el inciso 5 del artículo 2 de la Constitución, y los demás por la legislación pertinente
    - Información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la Administración Pública.
    - Información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal.

- Los activos de apoyo (sobre los cuales descansan los elementos primarios del alcance) de todo tipo:
  - Hardware
  - Software
  - Red y comunicaciones
  - Personal
  - Sitio
  - Estructura de la organización

  El listado de activos de apoyo, tanto de hardware como de software es el que figura en el ítem 1.2.3. del presente documento.

b. Valorización de activos

El siguiente paso luego de la identificación del activo es valorizar los activos. Esta tarea se inicia con acordar la escala que se debe utilizar y los criterios para asignar una ubicación particular en esa escala por cada activo en base a la valorización.

Criterios:

El criterio elegido para la valorización de activos son los costos incurridos debido a la pérdida de confidencialidad, integridad y disponibilidad como resultado de un incidente.

- **Confidencialidad**: Indica que la información del activo no puede ser vista por personal no autorizado.
- **Integridad**: El activo debe estar correcto y completo y debe ser protegido por cambios no autorizados, no previstos o accidentales.
- **Disponibilidad**: El activo debe estar disponible y utilizable en el momento que se necesite.

Escala:

En este caso se valorará una escala cuantitativa de acuerdo a los criterios de disponibilidad, integridad y confidencialidad, siendo el número 1 el de menor relevancia y el número 3 con el valor más relevante.

En la siguiente tabla se muestra los criterios y sus respectivos valores.

Tabla N° 39. Criterios definidos por la CGT para la valorización de activos de TI

Criterio	Valor en escala	Descripción
Disponibilidad	1	El activo debe estar disponible por lo menos 25% del tiempo que se necesite. No existe riesgo operacional, reputacional, ni legal si el activo de información se ha eliminado o no está disponible.
	2	El activo debe estar disponible por lo menos 50% del tiempo que se necesite. Si no lo estuviera o si fuese destruido puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe estar disponible el 100% del tiempo que se necesite. Si no lo estuviera o si fuese destruido ocasionará daños graves o hasta catastróficos para la organización, afectarán los intereses legales, operacionales o reputacionales, y causarán pérdidas financieras.
Integridad	1	El activo debe estar correcto y completo por lo menos el 25% de las veces que se necesite. No existe pérdidas financieras ni riesgo operacional, reputacional, ni legal.
	2	El activo debe ser correcto y completo al menos el 50% de las veces que se necesita. Puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe ser correcto y completo el 100% de las veces utilizadas. De no cumplir con lo anterior, puede causar daños graves o hasta catastróficos para la organización, y afectará los intereses legales, operacionales o reputacionales, además de pérdidas financieras significativas.

Confidencialidad	1	El activo es publicada o de conocimiento del público en general, por lo tanto, no existe ningún riesgo legal, reputacional, operacional, ni financiero.
	2	El activo podrá ser divulgado hacia los colaboradores. Si se cumple con lo anterior no será perjudicial para los intereses legales, reputacional, operacional, ni financiero.
	3	El activo contiene información altamente sensible. Su divulgación puede causar daños graves o hasta catastróficos, afectando los intereses legales, reputacionales, y financieros.

Como resultado de la identificación de activos se obtiene un listado de los activos involucrados en el alcance del SGSI relacionados con su respectivo propietario y con su valorización. El valor final del activo (Valor de Criticidad) será el promedio de los tres valores en base a los criterios (disponibilidad, integridad y confidencialidad).

En la tabla siguiente se describe el valor cualitativo promedio del activo (Valor de Criticidad):

Tabla N° 40. Escalas definidas por el CGT para la valoración cualitativa de los activos de TI

Valor promedio de activo	Descripción
3 – ALTO	Alto, contiene información confidencial y en muchos casos la disponibilidad debe ser del 100%.
2 – MEDIO	Medio, no contiene información sensible, pero debe cumplir con algunos criterios como disponibilidad e integridad.
1 – BAJO	Bajo, los activos ubicados en este valor promedio, son activos de carácter público.

En las siguientes tablas se muestran los resultados de la evaluación de los activos seleccionados de acuerdo con los criterios antes mencionados:

Tabla N° 41. Valorización de activos primarios

	propietario del activo	C	I	D	promedio	valor de criticidad
Activos primarios						
Gestión Administrativa	Oficina General de Administración	3	3	3	3	ALTO
Gestión operativa	División de recaudación y control de deuda	2	3	3	3	ALTO
Servicios públicos	División de servicios al administrado	2	2	2	2	MEDIO
Control Interno	Oficina de Control Interno	3	3	1	2	MEDIO
Información contenida en las bases de datos pertenecientes al CGT	Oficina de TI	2	3	3	3	ALTO
Información contenida en sistemas gubernamentales externos: SIGA y SIAF.	Oficina de TI	2	3	3	3	ALTO
Información contenida en el Correo electrónico institucional.	Oficina de TI	1	2	2	2	MEDIO
Información contenida en el Portal Web Institucional.	Oficina de TI	1	2	2	2	MEDIO
Información Confidencial del CGT	Oficina de Control Interno	3	3	2	3	ALTO

Tabla N° 42. Valorización de activos de apoyo

	propietario del activo	C	I	D	promedio	valor de criticidad
Activos de apoyo						
Servidores	Oficina de TI	3	3	3	3	ALTO
Computadoras de Escritorio	Jefe de Área	2	2	3	2	MEDIO
Equipo Portátil	Jefe de Área	1	2	2	2	MEDIO
Impresoras	Jefe de Área	-	-	2	2	MEDIO
Escáner	Jefe de Área	-	-	1	1	BAJO
Fuente de energía ininterrumpida	Oficina de TI	-	-	3	3	ALTO
Equipo de Refrigeración	Oficina de TI	-	-	3	3	ALTO
Otros medios impresos	Jefe de Área	-	-	2	2	MEDIO
Sistemas Operativos	Jefe de Área	2	2	3	2	MEDIO
Software en paquetes o software estándar	Jefe de Área	1	1	3	2	MEDIO
Herramienta de desarrollo	Oficina de TI	1	1	1	1	BAJO
Software antivirus	Jefe de Área	2	2	3	2	MEDIO
Aplicaciones empresariales	Jefe de Área	2	3	3	3	ALTO
Software gubernamental	Jefe de Área	2	3	3	3	ALTO
Otros	Jefe de Área	1	2	2	2	MEDIO
Equipos de comunicación central	Oficina de TI	2	3	3	3	ALTO
Equipos de comunicación secundario	Oficina de TI	2	2	3	2	MEDIO
Red física (cableado)	Oficina de TI	2	3	3	3	ALTO
Responsable de tomar decisiones	Gerencia CGT	3	3	2	3	ALTO
Usuarios	Jefe de Área	2	2	3	2	MEDIO
Personal de operaciones y mantenimiento	Oficina de TI	2	3	3	3	ALTO
Encargado en Desarrollo	Oficina de TI	2	2	2	2	MEDIO

Sala de Servidores	Oficina de TI	-	-	3	3	ALTO
Ubicación	Gerencia CGT	-	-	2	2	MEDIO
Entorno Externo	Gerencia CGT	-	-	2	2	MEDIO
Servicios esenciales	Gerencia CGT	-	-	3	3	ALTO
Gerencia CGT.	Gerencia CGT	3	2	2	2	MEDIO
Comité de Gestión de Seguridad de Información.	Gerencia CGT	3	2	2	2	MEDIO
Responsables del cumplimiento.	Gerencia CGT	2	2	2	2	MEDIO

En el presente análisis se ha definido que aquellos activos con un valor de criticidad Alto, son sobre los que se debe realizar el análisis de riesgos asociados, buscando establecer controles que los protejan de las amenazas presentes, asegurando la información que contienen o trasmiten.

4.4.2. Identificación de amenazas y vulnerabilidades

a. Identificación de amenazas por activo

A continuación se presenta un listado de amenazas posibles sobre los activos identificados

Tabla N° 43. Identificación de amenazas por activo

Amenazas	Activos Primarios		Activos de Apoyo					
	Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
[N] Desastres naturales								
[N.1] Fuego	√	√	√		√		√	
[N.2] Daños por agua	√	√	√		√		√	
[N.*] Desastres naturales	√	√	√		√		√	
[I] De origen industrial								
[I.1] Fuego	√	√	√		√		√	
[I.2] Daños por agua	√	√	√		√		√	
[I.3] Contaminación mecánica		√	√		√			
[I.4] Avería de origen físico o lógico	√	√	√	√	√			
[I.5] Corte del suministro eléctrico (5)	√	√	√		√			
[I.6] Condiciones inadecuadas de temperatura o humedad		√	√		√			
[I.7] Fallo de servicios de comunicaciones					√			

Amenazas	Activos Primarios		Activos de Apoyo					
	Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
[I.8] Degradación de los soportes de almacenamiento de la información		√						
[I.*] Desastres industriales		√	√		√	√	√	
[E] Errores y fallos no intencionados								
[E.1] Errores de configuración	√	√	√	√	√			
[E.2] Deficiencias en la organización						√		√
[E.3] Difusión de software dañino				√				
[E.4] Errores de [re-]encaminamiento				√	√			
[E.5] Errores de secuencia				√	√	√		
[E.6] Escapes de información		√		√	√	√		
[E.7] Alteración de la información	√	√						
[E.8] Introducción de información incorrecta		√						
[E.9] Destrucción de información		√						
[E.10] Divulgación de información		√						
[E.11] Caída del sistema por agotamiento de recursos	√		√		√			
[E.12] Pérdida de equipos			√	√	√			
[E.13] Indisponibilidad del personal						√		
[E.14] Errores de los usuarios	√	√	√	√	√	√		
[E.15] Errores del administrador (10)	√	√	√	√	√	√		
[E.16] Errores de monitorización (log)	√	√		√				

Amenazas	Activos Primarios		Activos de Apoyo					
	Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
[E.17] Vulnerabilidades de los programas (software)				√				
[E.18] Errores de mantenimiento / actualización de programas (software)				√				
[E.19] Errores de mantenimiento / actualización de equipos (hardware)			√					
[A] Ataques intencionados								
[A.1] Manipulación de la configuración	√	√	√	√	√			
[A.2] Uso no previsto	√	√	√	√	√		√	
[A.3] Difusión de software dañino				√				
[A.4] [Re-]encaminamiento de mensajes	√			√	√			
[A.5] Alteración de secuencia	√			√	√	√		
[A.6] Interceptación de información (escucha)		√	√	√	√	√		
[A.7] Modificación de la información		√						
[A.8] Introducción de falsa información		√						
[A.9] Destrucción la información		√						
[A.10] Divulgación de información		√						
[A.11] Denegación de servicio		√	√	√	√			
[A.12] Robo		√	√	√	√			
[A.13] Indisponibilidad del personal						√		
[A.14] Suplantación de la identidad del usuario	√	√		√	√			

Amenazas	Activos Primarios		Activos de Apoyo					
	Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
[A.15] Abuso de privilegios de acceso	√	√	√	√	√			
[A.16] Acceso no autorizado	√	√	√	√	√		√	
[A.17] Análisis de tráfico				√	√			
[A.18] Repudio	√	√						
[A.19] Manipulación de programas				√				
[A.20] Ataque destructivo		√	√		√	√	√	
[A.21] Ingeniería social						√		

b. Correlación de errores y ataques

Errores y amenazas constituyen frecuentemente las dos caras de la misma moneda: algo que le puede pasar a los activos sin intención o deliberadamente. Se pueden dar hasta tres combinaciones:

Las amenazas pueden producirse tanto por error como por ataque mal intencionado. Para ello, se ha elaborado unos catálogos de amenazas, tomando como referencia el catálogo de la metodología Magerit

Tabla N° 44. Catálogo general de amenazas

Número	Errores y fallos no intencionados	Ataque intencionados
*1	Errores de configuración	Manipulación de la configuración
*2	Deficiencias en la organización	Uso no previsto
*3	Difusión de software dañino	Difusión de software dañino
*4	Errores de [re-encaminamiento]	[Re-]encaminamiento de mensajes
*5	Errores de secuencia	Alteración de secuencia
*6	Escapes de información	Interceptación de información (escucha)
*7	Alteración de la información	Modificación de la información
*8	Introducción de información incorrecta	Introducción de falsa información
*9	Destrucción de información	Destrucción la información
*10	Divulgación de información	Divulgación de información
*11	Caída del sistema por agotamiento de recursos	Denegación de servicio
*12	Pérdida de equipos	Robo
*13	Indisponibilidad del personal	Indisponibilidad del personal

- Amenazas que sólo pueden ser errores, nunca ataques deliberados.

Tabla N° 45. Catálogo de amenazas del tipo Errores y fallos no intencionados

Número	Errores y fallos no intencionados
14	Errores de los usuarios
15	Errores del administrador
16	Errores de monitorización (log)
17	Vulnerabilidades de los programas (software)
18	Errores de mantenimiento / actualización de programas (software)
19	Errores de mantenimiento / actualización de equipos (hardware)

- Amenazas que nunca son errores: siempre son ataques deliberados.

Tabla N° 46. Catálogo de amenazas del tipo ataques mal intencionado

Número	Ataque intencionados
14	Suplantación de la identidad del usuario
15	Abuso de privilegios de acceso
16	Acceso no autorizado
17	Análisis de tráfico
18	Repudio
19	Manipulación de programas
20	Ataque destructivo
21	Ingeniería social

c. Identificación evaluación de vulnerabilidades

En la siguiente tabla se muestra vulnerabilidades agrupadas por tipo de activo:

Tabla N° 47. Catálogo de vulnerabilidades por tipo de activo

Tipos	Vulnerabilidades
Hardware	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento
	Falta de esquemas de reemplazo periódicos
	Susceptibilidad a la humedad, al polvo y a la suciedad
	Sensibilidad a la radiación electromagnética
	Falta de control eficiente del cambio de configuración
	Susceptibilidad a variaciones de voltaje
	Susceptibilidad a variaciones de temperatura
	Almacenamiento no protegido.
	Falta de cuidado al descartarlo
	Copia no controlada
Software	Pruebas al software inexistentes o insuficientes
	Errores conocidos en el software
	Computadoras personales sin programas antivirus
	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente
	Falta de evidencias de auditoría
	Asignación equivocada de derechos de acceso
	Desarrollo de software sin metodología
	Interfaz de usuario complicada
	Falta de documentación
	Configuración incorrecta de parámetros
	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios.
	Tablas de claves no protegidas.
	Mala administración de claves.
	Habilitación de servicios innecesarios.
	Especificaciones no claras o incompletas para los desarrolladores.
	Falta de control de cambios eficaz.
	Descarga y uso incontrolado de software.
	Falta de copias de respaldo.
Red	Líneas de comunicación no protegidas
	Tráfico delicado no protegido
	Punto de falla único.
	Falta de identificación y autentificación de emisor y destinatario.

Tipos	Vulnerabilidades
	Arquitectura de red insegura.
	Transferencia de claves en claro.
Personal	Ausencia de personal.
	Capacitación de seguridad insuficiente.
	Uso incorrecto del software y hardware.
	Falta de conciencia de seguridad.
	Falta de mecanismos de monitoreo.
	Trabajo no supervisado del personal externo o de limpieza.
	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería.
Sitio	Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones.
	Instalaciones sin extintores.
	Ubicaciones en un área susceptible a las inundaciones.
	Red inestable de energía eléctrica.
	Falta de protección física del edificio, puertas y ventanas.
	Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones.
Organización	Falta de revisiones regulares de la gestión
	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos
	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y / o terceros.
	Falta de auditorías regulares (supervisión).
	Falta de un procedimiento formal para el registro y baja de los usuarios.
	Falta de procedimiento de monitoreo de las instalaciones de procesamiento de la información.
	Falta de procedimientos de identificación y evaluación del riesgo
	Falta de informes de fallas registradas en los registros del administrador y del operador.
	Respuesta inadecuada del mantenimiento del servicio
	Falta de procedimiento de control de cambios
	Falta de proceso formal para autorización de información pública disponible
	Falta de asignación apropiada de responsabilidades de seguridad en la información
	Falta de planes de continuidad
	Falta de una política de uso de correos electrónicos
	Falta de procedimientos para introducir software en sistemas operativos
	Falta de procedimientos para manejo de la información clasificada
	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)

Tipos	Vulnerabilidades
	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información
	Falta de política formal sobre el uso de recursos informáticos.
	Inexistencia o insuficiencia de la política de “Escritorio despejado y pantalla despejada”
	Falta de autorización al acceso a las instalaciones de procesamiento de la información
	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad
	Falta de procedimientos para reportar debilidades en la seguridad de la información
	Falta de asignación apropiada de responsabilidades de seguridad en la información

4.4.3. Evaluación del impacto

Un incidente en la seguridad de la información puede impactar más que un activo o sólo una parte de un activo. El impacto se relaciona con el grado de éxito del incidente. Como consecuencia, existe una diferencia importante entre el valor del activo y el impacto que resulta del incidente.

Se considera que el impacto tiene ya sea un efecto inmediato (operativo) o futuro (empresarial) sobre la Confidencialidad, Integridad, Disponibilidad.

El impacto operativo inmediato es ya sea directo o indirecto.

a. Directo:

i. El valor de reemplazo financiero de activos perdidos o parte de los mismos.
ii. El costo de adquisición, configuración e instalación del nuevo activo o respaldo.
iii. El costo de las operaciones suspendidas debido al incidente hasta que el servicio proporcionado por el (los) activo (s) se restaure.
iv. Resultados del impacto en una ruptura de la seguridad de la información.

b. Indirecto:

i. Costo de oportunidad (se tiene que usar recursos financieros para reemplazar o reparar un activo que podría haber sido destinado a otra adquisición.
ii. El costo de las operaciones interrumpidas.
iii. Un mal uso potencial de la información obtenida a través de una ruptura de la seguridad.
iv. Violación de obligaciones estatutarias o regulatorias.
v. Violación de códigos de conducta éticos.

Como tal, la primera evaluación (sin controles de ningún tipo) estimará un impacto como muy cercano al (a los) valor (es) concernido (s) o a una combinación de los mismos. Para cualquier iteración siguiente sobre este (estos) activo (s), el impacto será diferente, normalmente mucho más bajo debido a la presencia y a la eficacia de los controles implementados.

Para este análisis se utilizará el siguiente formato:

Tabla N° 48. Formato para la evaluación de impacto

[código] descripción sucinta de la amenaza que puede pasar	
Tipos de activos que se pueden ver afectados por este tipo de amenazas	Impacto generado producto de la amenaza materializada, ordenados de más a menos relevante
Vulnerabilidad que la amenaza utiliza para que pueda materializarse.	

a. Desastres Naturales:

[N.1] Fuego

[N.1] Fuego	
Tipos de activos: · Procesos y actividades · Hardware. · Red y comunicaciones · Información · Sitio	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Susceptibilidad a variaciones de temperatura Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones. Falta de planes de continuidad Instalaciones sin extintores.	

[N.2] Daños por agua

[N.2] Daños por Agua	
Tipos de activos: · Procesos y actividades · Hardware. · Red y comunicaciones · Información · Sitio	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Falta de planes de continuidad Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones. Ubicaciones en un área susceptible a las inundaciones.	

[N.*] Desastres Naturales

[N.*] Desastres naturales	
Tipos de activos: · Procesos y actividades · Hardware. · Red y comunicaciones · Información · Sitio	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones. Falta de planes de continuidad. Instalaciones sin extintores.	

b. De tipo industrial:

[I.1] Fuego

[I.1] Fuego	
Tipos de activos: · Procesos y actividades · Hardware. · Red y comunicaciones · Información · Sitio	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones. Susceptibilidad a variaciones de temperatura Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones. Falta de planes de continuidad Instalaciones sin extintores.	

[I.2] Daños por agua

[I.2] Daños por Agua	
Tipos de activos: · Procesos y actividades · Hardware. · Red y comunicaciones · Información · Sitio	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Falta de planes de continuidad Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones. Ubicaciones en un área susceptible a las inundaciones	

[I.3] Contaminación mecánica

[I.3] Contaminación mecánica	
Tipos de activos: · Hardware. · Red y comunicaciones · Información	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Susceptibilidad a la humedad, al polvo y a la suciedad Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	

[I.4] Avería de origen físico o lógico

[I.4] Avería de origen físico o lógico	
Tipos de activos: · Procesos y actividades · Software. · Hardware. · Red y comunicaciones · Información	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Mantenimiento insuficiente / instalación fallida de medios de almacenamiento Uso incorrecto del software y hardware. Red inestable de energía eléctrica.	

[I.5] Corte del suministro eléctrico

[I.5] Corte del suministro eléctrico	
Tipos de activos: · Procesos y actividades · Hardware. · Red y comunicaciones · Información	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Red inestable de energía eléctrica. Susceptibilidad a variaciones de voltaje	

[I.6] Condiciones inadecuadas de temperatura o humedad

[I.6] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: · Hardware. · Red y comunicaciones · Información	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Susceptibilidad a la humedad, al polvo y a la suciedad Susceptibilidad a variaciones de temperatura	

[I.7] Fallo de servicios de comunicaciones

[I.7] Fallo de servicios de comunicaciones	
Tipos de activos: · Red y comunicaciones	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Falta de control eficiente del cambio de configuración Arquitectura de red insegura. Líneas de comunicación no protegidas Falta de una política de uso de correos electrónicos	

[I.8] Degradación de los soportes de almacenamiento de la información

[I.8] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: · Información	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Susceptibilidad a la humedad, al polvo y a la suciedad Susceptibilidad a variaciones de voltaje Susceptibilidad a variaciones de temperatura	

Almacenamiento no protegido. Copia no controlada Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente

[I.*] Desastres industriales

[I.*] Desastres industriales	
Tipos de activos: · Hardware · Red y comunicaciones · Información · Personal · Sitio	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Falta de planes de continuidad	

c. Errores y fallos no intencionados:

[E.*1] Errores de configuración

[E.*1] Errores de configuración	
Tipos de activos: · Procesos · Información · Software · Hardware. · Red y comunicaciones	Impacto sobre: 1. Disponibilidad 2. Integridad 3. Confidencialidad
Vulnerabilidad: Falta de control eficiente del cambio de configuración Configuración incorrecta de parámetros Habilitación de servicios innecesarios. Especificaciones no claras o incompletas para los desarrolladores. Transferencia de claves en claro. Uso incorrecto del software y hardware.	

[E.*2] Deficiencias en la organización

[E.*2] Deficiencias en la organización	
Tipos de activos: · Personal · Estructura organizacional	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Falta de un procedimiento formal para el registro y baja de los usuarios. Falta de procedimiento de monitoreo de las instalaciones de procesamiento de la información. Falta de auditorías regulares (supervisión). Falta de procedimientos de identificación y evaluación del riesgo Respuesta inadecuada del mantenimiento del servicio Falta de procedimiento de control de cambios Falta de proceso formal para autorización de información pública disponible Falta de asignación apropiada de responsabilidades de seguridad en la información Falta de planes de continuidad Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información Falta de política formal sobre el uso de recursos informáticos. Inexistencia o insuficiencia de la política de “Escritorio despejado y pantalla despejada”	

Falta de autorización al acceso a las instalaciones de procesamiento de la información Falta de revisiones regulares de la gestión Falta de procedimientos para reportar debilidades en la seguridad de la información Falta de asignación apropiada de responsabilidades de seguridad en la información

[E.*3] Difusión de software dañino

[E.*3] Difusión de software dañino	
Tipos de activos: · Software	Impacto sobre: 1. Disponibilidad 2. Integridad 3. Confidencialidad
Vulnerabilidad: Falta de conciencia de seguridad. Descarga y uso incontrolado de software. Falta de mecanismos de monitoreo. Falta de una política de uso de correos electrónicos. Computadoras personales sin programas antivirus. Falta de políticas para el uso correcto de mensajería.	

[E.*4] Errores de [re-]encaminamiento

[E.*4] Errores de [re-]encaminamiento	
Tipos de activos: · Software · Red y comunicaciones	Impacto sobre: 1. Confidencialidad
Vulnerabilidad: Falta de mecanismos de identificación y autentificación como la autentificación de usuarios. Líneas de comunicación no protegidas Tráfico delicado no protegido Arquitectura de red insegura. Ausencia de personal.	

[E.*5] Errores de secuencia

[E.*5] Errores de secuencia	
Tipos de activos: · Software · Red y comunicaciones · Personal	Impacto sobre: 1. Integridad
Vulnerabilidad: Falta de mecanismos de identificación y autentificación como la autentificación de usuarios. Líneas de comunicación no protegidas Tráfico delicado no protegido Arquitectura de red insegura. Punto de falla único. Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería.	

[E.*6] Escapes de información

[E.*6] Escapes de información	
Tipos de activos: · Información · Software · Red y comunicaciones · Personal	Impacto sobre: 1. Confidencialidad
Vulnerabilidad:	

Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería.

[E.*7] Alteración de la información

[E.*7] Alteración de la información	
Tipos de activos: · Procesos · Información	Impacto sobre: 1. Integridad
Vulnerabilidad: Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[E.*8] Introducción de información incorrecta

[E.*8] Introducción de información incorrecta	
Tipos de activos: · Información	Impacto sobre: 1. Integridad
Vulnerabilidad: Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[E.*9] Destrucción de información

[E.*9] Destrucción de información	
Tipos de activos: · Información	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente Uso incorrecto del software y hardware. Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros	

Falta de control eficiente del cambio de configuración

[E.*10] Divulgación de información

[E.*10] Divulgación de información	
Tipos de activos: · Información	Impacto sobre: 1. Confidencialidad
Vulnerabilidad: Uso incorrecto del software y hardware. Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[E.*11] Caída del sistema por agotamiento de recursos

[E.*11] Caída del sistema por agotamiento de recursos	
Tipos de activos: · Procesos · Hardware · Red y comunicaciones	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Uso incorrecto del software y hardware. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[E.*12] Pérdida de equipos

[E.*12] Pérdida de equipos	
Tipos de activos: · Hardware · Software · Red y comunicaciones	Impacto sobre: 1. Disponibilidad 2. Confidencialidad
Vulnerabilidad: Falta de esquemas de reemplazo periódicos Falta de planes de continuidad	

[E.*13] Indisponibilidad del personal

[E.*13] Indisponibilidad del personal	
Tipos de activos: · Personal	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Ausencia de personal. Falta de planes de continuidad	

[E.14] Errores de los usuarios

[E.14] Errores de los usuarios	
Tipos de activos: · Procesos · Información	Impacto sobre: 1. Integridad 2. Confidencialidad

· Software · Hardware · Red y comunicaciones · Personal	3. Disponibilidad
Vulnerabilidad: Falta de planes de continuidad Uso incorrecto del software y hardware. Falta de mecanismos de monitoreo. Trabajo no supervisado del personal externo o de limpieza. Capacitación de seguridad insuficiente. Falta de informes de fallas registradas en los registros del administrador y del operador.	

[E.15] Errores del administrador

[E.15] Errores del administrador	
Tipos de activos: · Procesos · Información · Software · Hardware · Red y comunicaciones · Personal	Impacto sobre: 1. Disponibilidad 2. Integridad 3. Confidencialidad
Vulnerabilidad: Falta de planes de continuidad Uso incorrecto del software y hardware. Falta de mecanismos de monitoreo. Capacitación de seguridad insuficiente. Falta de informes de fallas registradas en los registros del administrador y del operador. Falta de procedimiento de control de cambios	

[E.16] Errores de monitorización (log)

[E.16] Errores de monitorización (log)	
Tipos de activos: · Procesos · Información · Software · Estructura Organizacional	Impacto sobre: 1. Integridad
Vulnerabilidad: Falta de mecanismos de monitoreo. Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad Falta de revisiones regulares de la gestión	

[E.17] Vulnerabilidades de los programas (software)

[E.17] Vulnerabilidades de los programas (software)	
Tipos de activos: · Software	Impacto sobre: 1. Integridad 2. Disponibilidad 3. Confidencialidad
Vulnerabilidad: Pruebas al software inexistentes o insuficientes Errores conocidos en el software Falta de evidencias de auditoría Asignación equivocada de derechos de acceso Interfaz de usuario complicada Desarrollo de software sin metodología Falta de documentación Configuración incorrecta de parámetros	

Tablas de claves no protegidas. Mala administración de claves. Especificaciones no claras o incompletas para los desarrolladores. Falta de control de cambios eficaz.

[E.18] Errores de mantenimiento / actualización de programas (software)

[E.18] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: · Software	Impacto sobre: 1. Integridad 2. Disponibilidad
Vulnerabilidad: Pruebas al software inexistentes o insuficientes Errores conocidos en el software Falta de evidencias de auditoría Asignación equivocada de derechos de acceso Interfaz de usuario complicada Falta de documentación Configuración incorrecta de parámetros Tablas de claves no protegidas. Mala administración de claves. Especificaciones no claras o incompletas para los desarrolladores. Falta de control de cambios eficaz.	

[E.19] Errores de mantenimiento / actualización de equipos (hardware)

[E.19] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: · Hardware	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Mantenimiento insuficiente / instalación fallida de medios de almacenamiento Falta de esquemas de reemplazo periódicos	

d. Ataques intencionados:

[A.*1] Manipulación de la configuración

[A.*1] Manipulación de la configuración	
Tipos de activos: · Procesos · Información · Software · Hardware · Red y comunicaciones	Impacto sobre: 1. Integridad 2. Confidencialidad 3. Disponibilidad
Vulnerabilidad: Falta de control eficiente del cambio de configuración Configuración incorrecta de parámetros Habilitación de servicios innecesarios. Especificaciones no claras o incompletas para los desarrolladores. Transferencia de claves en claro. Uso incorrecto del software y hardware.	

[A.*2] Uso no previsto

[A.*2] Uso no previsto	
Tipos de activos: · Procesos · Información · Software · Hardware · Red y comunicaciones · Sitio	Impacto sobre: 1. Disponibilidad 2. Confidencialidad 3. Integridad
Vulnerabilidad: Uso incorrecto del software y hardware. Falta de conciencia de seguridad. Capacitación de seguridad insuficiente.	

[A.*3] Difusión de software dañino

[A.*3] Difusión de software dañino	
Tipos de activos: · Software	Impacto sobre: 1. Disponibilidad 2. Integridad 3. Confidencialidad
Vulnerabilidad: Falta de conciencia de seguridad. Descarga y uso incontrolado de software. Falta de mecanismos de monitoreo. Falta de una política de uso de correos electrónicos Computadoras personales sin programas antivirus Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería.	

[A.*4] [Re-]encaminamiento de mensajes

[A.*4] [Re-]encaminamiento de mensajes	
Tipos de activos: · Procesos · Software · Red y comunicaciones	Impacto sobre: 1. Confidencialidad
Vulnerabilidad: Falta de mecanismos de identificación y autentificación como la autentificación de usuarios. Líneas de comunicación no protegidas Tráfico delicado no protegido Arquitectura de red insegura. Ausencia de personal.	

[A.*5] Alteración de secuencia

[A.*5] Alteración de secuencia	
Tipos de activos: · Procesos · Software · Red y comunicaciones · Personal	Impacto sobre: 1. Integridad
Vulnerabilidad: Falta de mecanismos de identificación y autentificación como la autentificación de usuarios. Líneas de comunicación no protegidas Tráfico delicado no protegido Arquitectura de red insegura. Punto de falla único. Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería.	

[A.*6] Interceptación de información (escucha)

[A.*6] Interceptación de información (escucha)	
Tipos de activos: · Información · Software · Hardware · Red y comunicaciones · Personal	Impacto sobre: 1. Confidencialidad
Vulnerabilidad: Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería. Arquitectura de red insegura. Líneas de comunicación no protegidas	

[A.*7] Modificación de la información

[A.*7] Modificación de la información	
Tipos de activos: · Información	Impacto sobre: 1. Integridad
Vulnerabilidad: Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[A.*8] Introducción de falsa información

[A.*8] Introducción de falsa información	
Tipos de activos: · Información	Impacto sobre: 1. Integridad
Vulnerabilidad: Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[A.*9] Destrucción la información

[A.*9] Destrucción la información	
Tipos de activos: · Información	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente Uso incorrecto del software y hardware. Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[A.*10] Divulgación de información

[A.*10] Divulgación de información	
Tipos de activos: · Información	Impacto sobre: 1. Confidencialidad
Vulnerabilidad: Uso incorrecto del software y hardware. Almacenamiento no protegido. Falta de cuidado al descartarlo Copia no controlada Tablas de claves no protegidas. Habilitación de servicios innecesarios. Falta de copias de respaldo. Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente Transferencia de claves en claro. Trabajo no supervisado del personal externo o de limpieza. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[A.*11] Denegación de servicio

[A.*11] Denegación de servicio	
Tipos de activos: · Información · Hardware · Software · Red y comunicaciones	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Uso incorrecto del software y hardware. Configuración incorrecta de parámetros Falta de control eficiente del cambio de configuración	

[A.*12] Robo

[A.*12] Robo	
Tipos de activos: · Hardware · Software · Red y comunicaciones · Información	Impacto sobre: 1. Disponibilidad 2. Confidencialidad

Vulnerabilidad: Falta de esquemas de reemplazo periódicos Falta de planes de continuidad

[A.*13] Indisponibilidad del personal

[A.*13] Indisponibilidad del personal	
Tipos de activos: · Personal	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Ausencia de personal. Falta de planes de continuidad	

[A.14] Suplantación de la identidad del usuario

[A.14] Suplantación de la identidad del usuario	
Tipos de activos: · Procesos · Información · Software · Red y comunicaciones	Impacto sobre: 1. Confidencialidad 2. Integridad
Vulnerabilidad: Falta de mecanismos de identificación y autentificación como la autentificación de usuarios.	

[A.15] Abuso de privilegios de acceso

[A.15] Abuso de privilegios de acceso	
Tipos de activos: · Procesos · Información · Software · Hardware · Red y comunicaciones	Impacto sobre: 1. Confidencialidad 2. Integridad
Vulnerabilidad: Capacitación de seguridad insuficiente. Falta de conciencia de seguridad. Falta de mecanismos de monitoreo.	

[A.16] Acceso no autorizado

[A.16] Acceso no autorizado	
Tipos de activos: · Procesos · Información · Software · Hardware · Red y comunicaciones · Sitio	Dim1nsiones: 1. Confidencialidad 2. Integridad
Vulnerabilidad: Asignación equivocada de derechos de acceso Capacitación de seguridad insuficiente. Falta de conciencia de seguridad. Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones.	

[A.17] Análisis de tráfico

[A.17] Análisis de tráfico	
Tipos de activos: · Software · Red y comunicaciones	Impacto sobre: 1. Confidencialidad
Vulnerabilidad: Arquitectura de red insegura. Líneas de comunicación no protegidas Tráfico delicado no protegido	

[A.18] Repudio

[A.18] Repudio	
Tipos de activos: · Procesos · Información	Impacto sobre: 1. Integridad
Vulnerabilidad: Asignación equivocada de derechos de acceso Capacitación de seguridad insuficiente. Falta de conciencia de seguridad. Falta de mecanismos de monitoreo. Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones.	

[A.19] Manipulación de programas

[A.19] Manipulación de programas	
Tipos de activos: · Software	Impacto sobre: 1. Confidencialidad 2. Integridad
Vulnerabilidad: Desarrollo de software sin metodología Especificaciones no claras o incompletas para los desarrolladores	

[A.20] Ataque destructivo

[A.20] Ataque destructivo	
Tipos de activos: · Hardware · Red y comunicaciones · Información · Personal · Sitio	Impacto sobre: 1. Disponibilidad
Vulnerabilidad: Almacenamiento no protegido. Falta de protección física del edificio, puertas y ventanas Arquitectura de red insegura. Falta de mecanismos de monitoreo. Falta de copias de respaldo. Falta de planes de continuidad	

[A.21] Ingeniería social

[A.21] Ingeniería social	
Tipos de activos: · Personal	Impacto sobre: 1. Confidencialidad 2. Integridad 3. Disponibilidad
Vulnerabilidad:	

Capacitación de seguridad insuficiente. Falta de conciencia de seguridad. Falta de mecanismos de monitoreo. Falta de protección física del edificio, puertas y ventanas Arquitectura de red insegura. Falta de mecanismos de monitoreo. Falta de copias de respaldo. Falta de planes de continuidad

4.4.4. Evaluación del riesgo de alto nivel

La evaluación del riesgo de alto nivel considera los valores empresariales de los activos de información y los riesgos desde el punto de vista del negocio de la organización.

Sin embargo la evaluación del riesgo de alto nivel, como pocas veces se refiere a detalles de tecnología, es más apropiada para proveer controles organizacionales y no técnicos y aspectos de gestión de los controles técnicos o salvaguardas técnicas clave y comunes como los respaldos y los antivirus.

Una regla general que debe aplicarse es si la falta de seguridad en la información puede resultar en consecuencias adversas significativas para la organización, sus procesos empresariales o sus activos, luego se hace necesaria una segunda iteración de la evaluación del riesgo a nivel más detallado para identificar los riesgos potenciales.

a. **Inventario de riesgos en seguridad de la información de alto nivel**
   Tomando en cuenta los doce dominios de la norma NTP ISO/IEC 27001:2014 se definieron los siguientes riesgos:

Tabla N° 49. Inventario de riesgos en seguridad de la información de alto nivel

Dominio	Riesgo	Denominación
Dominio 1		A.5 Política de seguridad
	R1	A.5.1 Riesgo asociado a la Dirección de la Gerencia para la seguridad de la información.
		Inconvenientes presentados por la falta de proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos de la organización, las leyes y regulaciones relevantes.
Dominio 2		A.6 Organización de la seguridad de la información
	R2	A.6.1 Riesgo asociado a la organización interna
		Inconvenientes presentados por la falta de establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
Dominio 3		A.7 Seguridad de los recursos humanos

Dominio	Riesgo	Denominación
	R3	A.7.1 Riesgo asociado a la seguridad de los recursos humanos antes del empleo
		Inconvenientes presentados por la falta de asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.
	R4	A.7.2 Riesgo asociado a la seguridad de los recursos humanos durante el empleo
		Inconvenientes presentados por la falta de asegurar que todos los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.
	R5	A.7.3 Riesgo asociado a la seguridad de los recursos humanos terminación y cambio de empleo
		Inconvenientes presentados por la falta de proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.
Dominio 4		A.8 Gestión de activos
	R6	A.8.1 Riesgo asociado a la responsabilidad por los activos
		Inconvenientes presentados por la falta de identificar los activos de la organización y definir responsabilidades de protección apropiadas.
	R7	A.8.2 Riesgo asociado a la clasificación de la información
		Inconvenientes presentados por la falta de asegurar que la información reciba un nivel apropiado de protección en concordancia con su importancia para la organización.
	R8	A.8.3 Riesgo asociado al manejo de soporte de almacenamiento
		Inconvenientes presentados por la falta de prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.
Dominio 5		A.9 Control de acceso
	R9	A.9.1 Riesgo asociado al requerimiento del negocio para el control de acceso.
		Inconvenientes presentados por la falta de limitar el acceso a la información y a las instalaciones de procesamiento de la información.
	R10	A.9.2 Riesgo asociado a la gestión del acceso del usuario
		Inconvenientes presentados por la falta de asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.
	R11	A.9.3 Riesgo asociado a la responsabilidades de los usuarios
		Inconvenientes presentados por la falta de hacer que los usuarios respondan por la salvaguarda de su información de autenticación.
	R12	A.9.4 Riesgo asociado al control de acceso a sistema y aplicación.
		Inconvenientes presentados por la falta de prevenir el acceso no autorizado a los sistemas y aplicaciones.
Dominio 6		A.11 Seguridad física y ambiental
	R13	A.11.1 Riesgo asociado a las áreas seguras

Dominio	Riesgo	Denominación
		Inconvenientes presentados por la falta de impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.
	R14	A.11.2 Riesgo asociado a la seguridad de los equipos
		Inconvenientes presentados por la falta de prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.
Dominio 7		A.12 Seguridad de las operaciones
	R15	A.12.1 Riesgo asociado a los procedimientos y responsabilidades operativas
		Inconvenientes presentados por la falta de asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.
	R16	A.12.2 Riesgo asociado a la protección contra códigos maliciosos
		Inconvenientes presentados por la falta de asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.
	R17	A.12.3 Riesgo asociado al Respaldo (back-up)
		Inconvenientes presentados por la falta de proteger contra la pérdida de datos.
	R18	A.12.4 Riesgo asociado a registros y monitoreo
		Inconvenientes presentados por la falta de registrar eventos y generar evidencia.
	R19	A.12.5 Riesgo asociado al Control del software operacional
		Inconvenientes presentados por la falta de asegurar la integridad de los sistemas operacionales.
	R20	A.12.6 Riesgo asociado a la gestión de vulnerabilidad técnica.
		Inconvenientes presentados por la falta de prevenir la explotación de vulnerabilidades técnicas.
	R21	A.12.7 Riesgo asociado a las consideraciones para la auditoria de los sistemas de información.
		Inconvenientes presentados por la falta de minimizar el impacto de las actividades de auditoria en los sistemas operacionales.
Dominio 8		A.13 Seguridad de las comunicaciones
	R22	A.13.1 Riesgo asociado a la gestión de seguridad de la red.
		Inconvenientes presentados por la falta de asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.
	R23	A.13.2 Riesgo asociado a la transferencia de información
		Inconvenientes presentados por la falta de mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa.
Dominio 9		A.14 Riesgo asociado a la Adquisición, desarrollo y mantenimiento de sistemas

Dominio	Riesgo	Denominación
	R24	A.14.1 Riesgo asociado a los requisitos de seguridad de los sistemas de información
		Inconvenientes presentados por la falta de garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo.
	R25	A.14.2 Seguridad en los procesos de desarrollo y soporte
		Inconvenientes presentados por la falta de garantizar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
	R26	A.14.3 Riesgo asociado a los datos de prueba.
		Inconvenientes presentados por la falta de asegurar la protección de datos utilizados para las pruebas.
Dominio 10		A. 16 Gestión de incidentes de seguridad de la información
	R27	A.16.1 Riesgo asociado a la Gestión de incidentes e seguridad de la información y mejoras
		Inconvenientes presentados por la falta de asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.
Dominio 11		A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio
	R28	A.17.1 Riesgo asociado a la continuidad de seguridad de la información
		Inconvenientes presentados por la falta de la continuidad de seguridad de la información al no estar embebida en los sistemas de gestión de continuidad del negocio de la organización.
	R29	A.17.2 Riesgo asociado a las redundancias
		Inconvenientes presentados por la falta de asegurar la disponibilidad de las instalaciones y procesamiento de la información.
Dominio 12		A.18 Cumplimiento
	R30	A.18.1 Riesgo asociado al cumplimiento con requerimientos legales y contractuales
		Inconvenientes presentados por la falta de evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.
	R31	A.18.2 Riesgo asociado a las revisiones de seguridad de la información
		Inconvenientes presentados por la falta de asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.

b. Matrices de riesgos en seguridad de la información de alto nivel

Las siguientes tablas relacionan los riesgos identificados con los activos primarios y de apoyo del CGT.

Tabla N° 50. Matriz de evaluación de riesgos en seguridad de la información de alto nivel

MATRIZ DE RIESGOS VS ACTIVOS										
RIESGOS			ACTIVOS PRIMARIOS		ACTIVOS DE APOYO					
			Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
Dominio 1		A.5 Política de seguridad								
	R1	A.5.1 Riesgo asociado a la Dirección de la Gerencia para la seguridad de la información.						√		√
Dominio 2		A.6 Organización de la seguridad de la información								
	R2	A.6.1 Riesgo asociado a la organización interna	√	√				√		√
Dominio 3		A.7 Seguridad de los recursos humanos								
	R4	A.7.1 Riesgo asociado a la seguridad de los recursos humanos antes del empleo	√					√		√
	R5	A.7.2 Riesgo asociado a la seguridad de los recursos humanos durante el empleo	√					√		√
	R5	A.7.3 Riesgo asociado a la seguridad de los recursos humanos terminación y cambio de empleo	√					√		√
Dominio 4		A.8 Gestión de activos								
	R6	A.8.1 Riesgo asociado a la responsabilidad por los activos								√
	R7	A.8.2 Riesgo asociado a la clasificación de la información	√							√
	R8	A.8.3 Riesgo asociado al manejo de soporte de almacenamiento		√						√
Dominio 5		A.9 Control de acceso								

MATRIZ DE RIESGOS VS ACTIVOS										
RIESGOS			ACTIVOS PRIMARIOS		ACTIVOS DE APOYO					
			Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
		A.9.1 Riesgo asociado al requerimiento del negocio para el control de acceso.	√	√	√	√	√	√	√	√
		A.9.2 Riesgo asociado a la gestión del acceso del usuario	√	√	√	√	√	√	√	√
		A.9.3 Riesgo asociado a la responsabilidades de los usuarios						√		√
		A.9.4 Riesgo asociado al control de acceso a sistema y aplicación.		√		√	√	√		√
Dominio 6		A.11 Seguridad física y ambiental								
	R13	A.11.1 Riesgo asociado a las áreas seguras							√	
	R14	A.11.2 Riesgo asociado a la seguridad de los equipos			√		√	√	√	
Dominio 7		A.12 Seguridad de las operaciones								
	R15	A.12.1 Riesgo asociado a los procedimientos y responsabilidades operativas	√					√		√
	R16	A.12.2 Riesgo asociado a la protección contra códigos maliciosos		√		√		√		√
	R17	A.12.3 Riesgo asociado al Respaldo	√	√				√		√
	R18	A.12.4 Riesgo asociado a registros y monitoreo	√					√		√
	R19	A.12.5 Riesgo asociado al Control del software operacional		√	√	√	√			√
	R20	A.12.6 Riesgo asociado a la gestión de vulnerabilidad técnica.			√	√	√	√		√

MATRIZ DE RIESGOS VS ACTIVOS										
RIESGOS			ACTIVOS PRIMARIOS		ACTIVOS DE APOYO					
			Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
	R21	A.12.7 Riesgo asociado a las consideraciones para la auditoria de los sistemas de información.	√	√	√	√	√	√	√	√
Dominio 8		A.13 Seguridad de las comunicaciones								
	R22	A.13.1 Riesgo asociado a la gestión de seguridad de la red.		√		√	√	√		√
	R23	A.13.2 Riesgo asociado a la transferencia de información		√			√			√
Dominio 9		A.14 Adquisición, desarrollo y mantenimiento de sistemas								
	R24	A.14.1 Riesgo asociado a los requisitos de seguridad de los sistemas de información				√				√
	R25	A.14.2 Seguridad en los procesos de desarrollo y soporte	√	√		√				√
	R26	A.14.3 Riesgo asociado a los datos de prueba.		√		√	√			√
Dominio 10		A. 16 Gestión de incidentes de seguridad de la información								
	R27	A.16.1 Riesgo asociado a la Gestión de incidentes e seguridad de la información y mejoras								√
Dominio 11		A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio								
	R28	A.17.1 Riesgo asociado a la continuidad de seguridad de la información	√	√	√	√	√	√	√	√

MATRIZ DE RIESGOS VS ACTIVOS										
RIESGOS			ACTIVOS PRIMARIOS		ACTIVOS DE APOYO					
			Procesos y Actividades	Información	Hardware	Software	Red y comunicaciones	Personal	Sitio	Estructura organizacional
	R29	A.17.2 Riesgo asociado a las redundancias		√		√		√	√	√
Dominio 12		A.18 Cumplimiento								
	R30	A.18.1 Riesgo asociado al cumplimiento con requerimientos legales y contractuales	√	√	√	√		√		√
	R31	A.18.2 Riesgo asociado a las revisiones de seguridad de la información	√	√						√

La siguiente tabla muestran la evaluación cualitativa del riesgo en base a la probabilidad e impacto teniendo en cuenta una escala de 5X5, donde 1: poco impacto o poca probabilidad y 5: gran impacto o probabilidad.

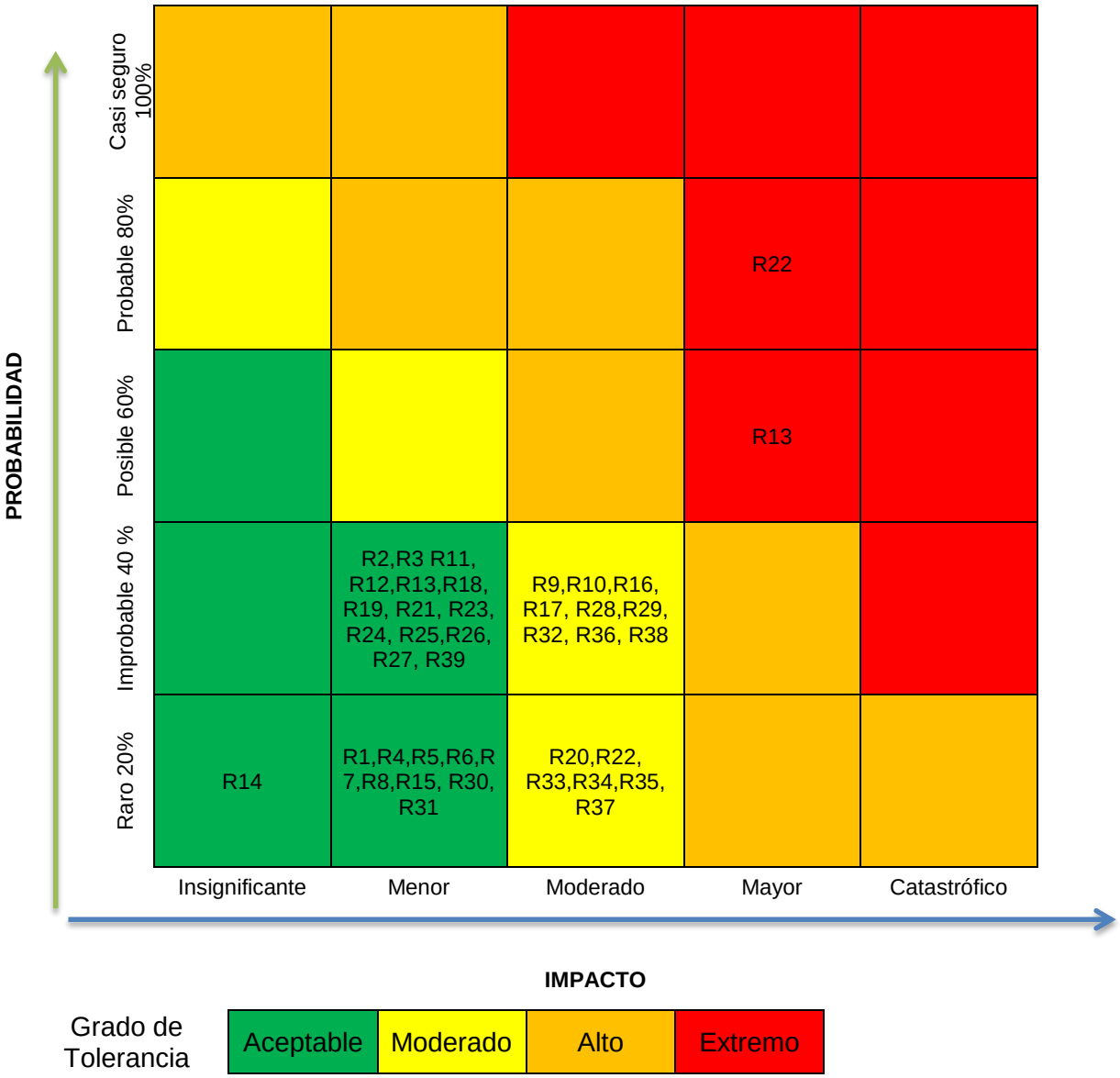
Se evaluó la probabilidad de ocurrencia y grado de impacto de los riesgos definidos de manera general.

Tabla N° 51. Matriz general de riesgos (probabilidad x impacto)

Riesgo			Probabilidad						Impacto				
			1	2	3	4	5		1	2	3	4	5
Dominio 1		A.5 Política de seguridad											
	R1	A.5.1 Riesgo asociado a la Dirección de la Gerencia para la seguridad de la información.			X						X		
Dominio 2		A.6 Organización de la seguridad de la información											
	R2	A.6.1 Riesgo asociado a la organización interna			X					X			
Dominio 3		A.7 Seguridad de los recursos humanos											
	R3	A.7.1 Riesgo asociado a la seguridad de los recursos humanos antes del empleo		X						X			
	R4	A.7.2 Riesgo asociado a la seguridad de los recursos humanos durante el empleo		X						X			
	R5	A.7.3 Riesgo asociado a la seguridad de los recursos humanos terminación y cambio de empleo		X						X			
Dominio 4		A.8 Gestión de activos											
	R6	A.8.1 Riesgo asociado a la responsabilidad por los activos		X						X			
	R7	A.8.2 Riesgo asociado a la clasificación de la información		X						X			
	R8	A.8.3 Riesgo asociado al manejo de soporte de almacenamiento		X						X			
Dominio 5		A.9 Control de acceso											
	R9	A.9.1 Riesgo asociado al requerimiento del negocio para el control de acceso.		X							X		
	R10	A.9.2 Riesgo asociado a la gestión del acceso del usuario	X								X		
	R11	A.9.3 Riesgo asociado a la responsabilidades de los usuarios				X					X		
	R12	A.9.4 Riesgo asociado al control de acceso a sistema y aplicación.			X					X			
Dominio 6		A.11 Seguridad física y ambiental											
	R13	A.11.1 Riesgo asociado a las áreas seguras			X							X	

Riesgo			Probabilidad						Impacto				
			1	2	3	4	5		1	2	3	4	5
	R14	A.11.2 Riesgo asociado a la seguridad de los equipos		X								X	
Dominio 7		A.12 Seguridad de las operaciones											
	R15	A.12.1 Riesgo asociado a los procedimientos y responsabilidades operativas		X						X			
	R16	A.12.2 Riesgo asociado a la protección contra códigos maliciosos				X					X		
	R17	A.12.3 Riesgo asociado al Respaldo (back-up)		X							X		
	R18	A.12.4 Riesgo asociado a registros y monitoreo			X						X		
	R19	A.12.5 Riesgo asociado al Control del software operacional			X					X			
	R20	A.12.6 Riesgo asociado a la gestión de vulnerabilidad técnica.			X						X		
	R21	A.12.7 Riesgo asociado a las consideraciones para la auditoria de los sistemas de información.		X							X		
Dominio 8		A.13 Seguridad de las comunicaciones											
	R22	A.13.1 Riesgo asociado a la gestión de seguridad de la red.				X						X	
	R23	A.13.2 Riesgo asociado a la transferencia de información			X						X		
Dominio 9		A.14 Riesgo asociado a la Adquisición, desarrollo y mantenimiento de sistemas											
	R24	A.14.1 Riesgo asociado a los requisitos de seguridad de los sistemas de información			X						X		
	R25	A.14.2 Seguridad en los procesos de desarrollo y soporte	X							X			
	R26	A.14.3 Riesgo asociado a los datos de prueba.		X						X			
Dominio 10		A. 16 Gestión de incidentes de seguridad de la información											
	R27	A.16.1 Riesgo asociado a la Gestión de incidentes e seguridad de la información y mejoras			X						X		
Dominio 11		A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio											
	R28	A.17.1 Riesgo asociado a la continuidad de seguridad de la información		X								X	
	R29	A.17.2 Riesgo asociado a las redundancias		X							X		
Dominio 12		A.18 Cumplimiento											

Riesgo			Probabilidad						Impacto				
			1	2	3	4	5		1	2	3	4	5
	R30	A.18.1 Riesgo asociado al cumplimiento con requerimientos legales y contractuales	X									X	
	R31	A.18.2 Riesgo asociado a las revisiones de seguridad de la información			X						X		



Grado de Tolerancia	Aceptable	Moderado	Alto	Extremo

Figura N° 20. Mapa de calor de los riesgos identificados
Fuente: Desarrollo Propio

De las matrices desarrolladas podemos concluir que los riesgos afectan de manera similar tanto a los activos primarios como de apoyo, por lo que al ocurrir un evento no deseado sobre alguno de ellos, se alterará su funcionamiento normal de manera similar para todos los procesos.

Otras de las consideraciones que se puede desprender de las matrices, es que la mayoría de los riesgos se ubican en la zona moderada y zona aceptable, son dos riesgos los que se ubican en la zona de riesgo extremo, lo que indica que se viene haciendo los esfuerzos necesarios para tratar el riesgo mediante la implementación de controles, aunque estos no estén implementados de la manera adecuada.

c. Criterio de aceptación

Del análisis de los mapas de riesgos anteriores se puede concluir que se han registrado 15 riesgos en la Zona Tolerancia Moderada donde los riesgos se encuentran controlados pero debe continuarse su evaluación periódica.

También se han registrado 25 riesgos en la Zona de Tolerancia Aceptable en donde se puede apreciar que los controles han minimizado el impacto de los riesgos, pero no se debe dejar de evaluarlos. Así mismo se encontraron dos riesgos en la Zona Extrema, estos deberían ser evaluados, sin embargo para un mayor estudio de estos es necesario realizar una evaluación detallada del riesgo para su posterior tratamiento.

d. Evaluación detallada del riesgo en seguridad de la información

El proceso de evaluación detallada del riesgo en seguridad de la información incluye una identificación y valorización profunda de los activos, la evaluación de amenazas a esos activos y la evaluación de vulnerabilidades. Los resultados de esas actividades se utilizan entonces para evaluar los riesgos y luego identificar el tratamiento del riesgo.

Tomando en cuenta los activos primarios y de apoyo, se identificaran dos tipos de riesgos:

Código del Riesgo	Denominacion
RP	Riesgos que afectan a los activos primarios del CGT.
RA	Riesgos que afectan a los activos de apoyo del CGT.

A partir del cuadro anterior se identificaron los riesgos y luego se evaluó la probabilidad de ocurrencia y su grado de impacto.

Tabla N° 52. Matriz detalla de riesgos que afectan a los activos primarios

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
Gestión administrativa	[E.2] Deficiencias de la organización	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento Uso incorrecto de software y hardware	RP1	Riesgo asociado a interrupción en el proceso de Gestión administrativa del CGT originado por fallos en los equipos y/o en los programas	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[I.5] Corte de suministro eléctrico	Red de energía eléctrica inestable Variaciones de voltaje	RP2	Riesgo asociado a interrupción en el proceso de Gestión administrativa del CGT debido a fallas eléctricas	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[E.7] Alteración de la información	Almacenamiento no protegido Copia no controlada Falta de un control eficiente del cambio de configuración	RP3	Riesgo asociado a interrupción en el proceso de Gestión administrativa del CGT debido a alteraciones de la información	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[E.11] Caída del sistema por agotamiento de recursos	Uso incorrecto de software y hardware Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración	RP4	Riesgo asociado a interrupción en el proceso de Gestión administrativa del CGT debido a la saturación de los sistemas informáticos	3	POSIBLE	5	CATASTROFICO	15	RIESGO EXTREMO
	[E.14] Errores de los usuarios	Uso incorrecto de software y hardware Mecanismos de monitoreo deficientes Capacitación en seguridad insuficiente Ausencia de informes de fallas registradas en los los registros del administrador y los operadores	RP5	Riesgo asociado a interrupción en el proceso de Gestión administrativa del CGT debido a las equivocaciones de los usuarios cuando usan los equipos o sistemas informáticos	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
Gestión operativa	[I.4] Avería de origen físico y lógico	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento Uso incorrecto de software y hardware	RP6	Riesgo asociado a interrupción en el proceso de Gestión Operativa originado por fallos en los equipos y/o en los programas	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[I.5] Corte de suministro eléctrico	Red de energía eléctrica inestable Variaciones de voltaje	RP7	Riesgo asociado a interrupción en el proceso de Gestión operativaT debido a fallas eléctricas	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[E.7] Alteración de la información	Almacenamiento no protegido Copia no controlada Falta de un control eficiente del cambio de configuración	RP8	Riesgo asociado a interrupción en el proceso de Gestión Operativa debido a alteraciones de la información	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[E.11] Caída del sistema por agotamiento de recursos	Uso incorrecto de software y hardware Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración	RP9	Riesgo asociado a interrupción en el proceso de Gestión Operativa debido a la saturación de los sistemas informáticos	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[E.14] Errores de los usuarios	Uso incorrecto de software y hardware Mecanismos de monitoreo deficientes Capacitación en seguridad insuficiente Ausencia de informes de fallas registradas en los los registros del administrador y los operadores Inexistencia de Planes de continuidad	RP10	Riesgo asociado a interrupción en el proceso de Gestión Operativa debido a las equivocaciones de los usuarios cuando usan los equipos o sistemas informáticos	4	PROBABLE	4	SIGNIFICATIVO	16	RIESGO EXTREMO
Información contenida en las base de datos del CGT	[I.8] Degradación de los soportes de almacenamiento de la información	Susceptibilidad a la humedad, al polvo y a la suciedad Variaciones de voltaje Almacenamiento no protegido Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	RP11	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a la degradación de los soportes de almacenamiento con el paso del tiempo	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
	[E.6] Escapes de información	Almacenamiento no protegido Copia no controlada Habilitación de servicios innnecesarios Falta de copias de respaldo Transferencia de claves	RP12	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a que la información llega accidentalmente a usuarios sin autorización	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[E.8] Introducción de información incorrecta	Almacenamiento no protegido Tablas claves no protegidas Falta de un control eficiente del cambio de configuración	RP13	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a la introducción incorrecta de la información	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[E.10] Divulgación de la información	Uso incorrecto de software y hardware Almacenamiento no protegido Habilitación de servicios innnecesarios	RP14	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a su divulgación por alguna indisecreción o revelación	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[E.14] Errores de los usuarios	Uso incorrecto de software y hardware Mecanismos de monitoreo deficientes Capacitación en seguridad insuficiente Ausencia de informes de fallas registradas en los los registros del administrador y los operadores	RP15	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a equivocaciones de los usuarios cuando usan equipos o sistemas informáticos	4	PROBABLE	4	SIGNIFICATIVO	16	RIESGO EXTREMO
	[A.2] Uso no previsto	Uso incorrecto de software y hardware Falta de conciencia del personal Capacitación en seguridad insuficiente	RP16	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a la utilización de los recursos informáticos para fines no previstos	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[A.7] Modificación de la información	Almacenamiento no protegido Copia no controlada Configuración incorrecta de parámetros	RP17	Riesgo asociado a la pérdida o daño de la información contenida en las BD a causa de alteraciones, con ánimo de obtener beneficio o causar perjuicio	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[A.8] Introducción de falsa información	Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración Copia no controlada	RP18	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a la introducción de información falsa	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[A.12] Robo	Acceso físico no autorizado Acceso no autorizado a la infraestructura informática Falta de políticas de seguridad	RP19	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a la sustracción de equipos informáticos	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[A.16] Acceso no autorizado	Asignación equivocada de derechos de acceso Capacitación en seguridad insuficiente Falta de conciencia del personal Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas	RP20	Riesgo asociado a la pérdida o daño de la información contenida en las BD debido a accesos no autorizados	4	PROBABLE	4	SIGNIFICATIVO	16	RIESGO EXTREMO
Información contenida en sistemas gubernamentales externos: SIGA, SIAF	[I.8] Degradación de los soportes de almacenamiento de la información	Susceptibilidad a la humedad, al polvo y a la suciedad Variaciones de voltaje Almacenamiento no protegido Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	RP21	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a la degradación de los soportes de almacenamiento con el paso del tiempo	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
	[E.6] Escapes de información	Almacenamiento no protegido Copia no controlada Habilitación de servicios innnecesarios Falta de copias de respaldo Transferencia de claves	RP22	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a que la información llega accidentalmente a usuarios sin autorización	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
	[E.8] Introducción de información incorrecta	Almacenamiento no protegido Tablas claves no protegidas	RP23	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a la introducción incorrecta de la información	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
		Falta de un control eficiente del cambio de configuración								
	[E.10] Divulgación de la información	Uso incorrecto de software y hardware	RP24	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a su divulgación por alguna indisecreción o revelación	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Almacenamiento no protegido								
		Habilitación de servicios innnecesarios								
	[E.14] Errores de los usuarios	Uso incorrecto de software y hardware	RP25	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a equivocaciones de los usuarios cuando usan equipos o sistemas informáticos	4	PROBABLE	4	SIGNIFICATIVO	16	RIESGO EXTREMO
		Mecanismos de monitoreo deficientes								
		Capacitación en seguridad insuficiente								
		Ausencia de informes de fallas registradas en los los registros del administrador y los operadores								
	[A.2] Uso no previsto	Uso incorrecto de software y hardware	RP26	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a la utilización de los recursos informáticos para fines no previstos	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Falta de conciencia del personal								
		Capacitación en seguridad insuficiente								
	[A.7] Modificación de la información	Almacenamiento no protegido	RP27	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales a causa de su alteración con ánimo de obtener beneficio o causar perjuicio	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
		Copia no controlada								
		Configuración incorrecta de parámetros								
	[A.8] Introducción de falsa información	Configuración incorrecta de parámetros	RP28	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a la introducción de información falsa	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Falta de un control eficiente del cambio de configuración								
		Copia no controlada								
	[A.12] Robo	Acceso físico no autorizado	RP29	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a la sustracción de equipos informáticos	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
		Acceso no autorizado a la infraestructura informática								
		Falta de políticas de seguridad								
	[A.16] Acceso no autorizado	Asignación equivocada de derechos de acceso	RP30	Riesgo asociado a la pérdida o daño de la información contenida en los sistemas gubernamentales debido a accesos no autorizados	4	PROBABLE	4	SIGNIFICATIVO	16	RIESGO EXTREMO
		Capacitación en seguridad insuficiente								
		Falta de conciencia del personal								

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
		Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas								
Información confidencial del CGT	[I.8] Degradación de los soportes de almacenamiento de la información	Susceptibilidad a la humedad, al polvo y a la suciedad	RP31	Riesgo asociado a la pérdida o daño de la información confidencial debido a la degradación de los soportes de almacenamiento con el paso del tiempo	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
		Variaciones de voltaje								
		Variaciones de temperatura								
		Almacenamiento no protegido								
		Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente								
	[E.6] Escapes de información	Almacenamiento no protegido	RP32	Riesgo asociado a la pérdida o daño de la información confidencial debido a que la información llega accidentalmente a usuarios sin autorización	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
		Copia no controlada								
		Habilitación de servicios innnecesarios								
		Falta de copias de respaldo								
		Transferencia de claves								
	[E.8] Introducción de información incorrecta	Almacenamiento no protegido	RP33	Riesgo asociado a la pérdida o daño de la información confidencial debido a la introducción incorrecta de la información	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
		Tablas claves no protegidas								
		Falta de un control eficiente del cambio de configuración								
	[E.10] Divulgación de la información	Uso incorrecto de software y hardware	RP34	Riesgo asociado a la pérdida o daño de la información confidencial debido a su divulgación por alguna indisecreción o revelación	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
		Almacenamiento no protegido								
		Habilitación de servicios innnecesarios								
	[E.14] Errores de los usuarios	Uso incorrecto de software y hardware	RP35	Riesgo asociado a la pérdida o daño de la información confidencial debido a equivocaciones de los usuarios cuando usan equipos o sistemas informáticos	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Mecanismos de monitoreo deficientes								
		Capacitación en seguridad insuficiente								
		Ausencia de informes de fallas registradas en los los registros del administrador y los operadores								
	[A.2] Uso no previsto	Uso incorrecto de software y hardware	RP36	Riesgo asociado a la pérdida o daño de la información confidencial debido a la utilización de los recursos informáticos para fines no previstos	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Falta de conciencia del personal								
		Capacitación en seguridad insuficiente								
	[A.7] Modificación de la información	Almacenamiento no protegido	RP37	Riesgo asociado a la pérdida o daño de la información confidencial a causa de su alteración con ánimo de obtener beneficio o causar perjuicio	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
		Copia no controlada								
		Configuración incorrecta de parámetros								
		Configuración incorrecta de parámetros	RP38		1	RARO	5	CATASTROFICO	5	RIESGO BAJO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[A.8] Introducción de falsa información	Falta de un control eficiente del cambio de configuración		Riesgo asociado a la pérdida o daño de la información confidencial debido a la introducción de información falsa						
		Copia no controlada								
	[A.12] Robo	Acceso físico no autorizado	RP39	Riesgo asociado a la pérdida o daño de la información confidencial debido a la sustracción de equipos informáticos	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
		Acceso no autorizado a la infraestructura informática								
		Falta de políticas de seguridad								
	[A.16] Acceso no autorizado	Asignación equivocada de derechos de acceso	RP40	Riesgo asociado a la pérdida o daño de la información confidencial debido a accesos no autorizados	2	IMPROBABLE	5	CATASTROFICO	10	RIESGO ALTO
		Capacitación en seguridad insuficiente								
		Falta de conciencia del personal								
		Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas								

Tabla N° 53. Matriz detalla de riesgos que afectan a los activos de apoyo

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
Servidores	[I.3] Contaminación mecánica	Susceptibilidad a la humedad, al polvo y a la suciedad Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA1	Riesgo asociado a los fallos de los servidores debido a la contaminación mecánica	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[I.4] Avería de origen físico y lógico	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento Uso incorrecto de software y hardware Red de energía eléctrica inestable	RA2	Riesgo asociado a los fallos de los servidores debido a alguna avería física o lógica	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[I.5] Corte de suministro eléctrico	Red de energía eléctrica inestable Variaciones de voltaje	RA3	Riesgo asociado a los fallos de los servidores debido a corte de suministro de energía eléctrica	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[E.1] Errores de configuración	Falta de un control eficiente del cambio de configuración Transferencia de claves Uso incorrecto de software y hardware	RA4	Riesgo asociado a los fallos de los servidores debido errores de configuración	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[E.11] Caída del sistema por agotamiento de recursos	Uso incorrecto de software y hardware Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración	RA5	Riesgo asociado a los fallos de los servidores debido a saturación de los sistemas informáticos	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[E.14] Errores de los usuarios	Uso incorrecto de software y hardware Mecanismos de monitoreo deficientes Capacitación en seguridad insuficiente Ausencia de informes de fallas registradas en los los registros del administrador y los operadores	RA6	Riesgo asociado a los fallos de los servidores debido errores de los usuarios	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
	[E.19] Errores del administrador	Uso incorrecto de software y hardware Mecanismos de monitoreo deficientes Capacitación en seguridad insuficiente Ausencia de informes de fallas registradas en los los registros del administrador y los operadores	RA7	Riesgo asociado a los fallos de los servidores debido a errores del administrador	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
	[E.19] Errores de mantenimiento / Actualización de equipos (hardware)	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA8	Riesgo asociado a los fallos de los servidores debido a errores de mantenimiento y actualización de equipos	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[A.11] Denegación de servicio	Uso incorrecto de software y hardware Falta de un control eficiente del cambio de configuración	RA9	Riesgo asociado a los fallos de los servidores debido a alguna denegación de servicio	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
	[A.12] Robo	Acceso físico no autorizado Acceso no autorizado a la infraestructura informática Falta de políticas de seguridad	RA10	Riesgo asociado a los fallos de los servidores debido a la sustracción de algún equipo	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
Fuente de energía ininterrumpida	[I.3] Contaminación mecánica	Susceptibilidad a la humedad, al polvo y a la suciedad Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA11	Riesgo asociado a los fallos de los equipos de alimentación de energía debido a contaminación mecánica	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[I.5] Corte de suministro eléctrico	Red de energía eléctrica inestable Variaciones de voltaje	RA12	Riesgo asociado a los fallos de los equipos de alimentación de energía debido fallos eléctricos	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[E.19] Errores de mantenimiento / Actualización de equipos (hardware)	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA13	Riesgo asociado a los fallos de los equipos de alimentación de energía debido errores de mantenimiento o o en los procedimientos de actualización de equipos	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[A.11] Denegación de servicio	Uso incorrecto de software y hardware Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración	RA14	Riesgo asociado a los fallos de los equipos de alimentación de energía debido a alguna denegación de servicio	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[A.12] Robo	Acceso físico no autorizado Acceso no autorizado a la infraestructura informática Falta de políticas de seguridad	RA15	Riesgo asociado a los fallos de los equipos de alimentación de energía debido a la sustracción de equipos	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
Equipos de refrigeración	[I.3] Contaminación mecánica	Susceptibilidad a la humedad, al polvo y a la suciedad Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA16	Riesgo asociado a los fallos de los equipos de refrigeración debido a contaminación mecánica	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
	[I.5] Corte de suministro eléctrico	Red de energía eléctrica inestable Variaciones de voltaje	RA17	Riesgo asociado a los fallos de los equipos de refrigeración debido fallos eléctricos	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[E.19] Errores de mantenimiento / Actualización de equipos (hardware)	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA18	Riesgo asociado a los fallos de los equipos de refrigeración debido errores de mantenimiento o o en los procedimientos de actualización de equipos	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
	[A.11] Denegación de servicio	Uso incorrecto de software y hardware Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración	RA19	Riesgo asociado a los fallos de los equipos de refrigeración debido a alguna denegación de servicio	1	RARO	3	MODERADO	3	RIESGO BAJO
	[A.12] Robo	Acceso físico no autorizado Acceso no autorizado a la infraestructura informática Falta de políticas de seguridad	RA20	Riesgo asociado a los fallos de los equipos de refrigeración debido a la sustracción de equipos	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
Aplicaciones empresariales	[I.4] Avería de origen físico y lógico	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento Uso incorrecto de software y hardware	RA21	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a defectos de origen físico o lógico durante su funcionamiento	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[E.1] Errores de configuración	Falta de un control eficiente del cambio de configuración Configuración incorrecta de parámetros Habilitación de servicios innnecesarios Uso incorrecto de software y hardware	RA22	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a la introducción de datos de configuración en forma errónea	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[E.3] Difusión de software dañino	Falta de conciencia del personal Descarga y uso incontrolado de software Mecanismos de monitoreo deficientes Falta de una política de uso de correo electrónico Computadoras personales sin programas antivirus	RA23	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a la propagación de algún software dañino	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[E.19] Errores del administrador	Uso incorrecto de software y hardware Mecanismos de monitoreo deficientes Capacitación en seguridad insuficiente Ausencia de informes de fallas registradas en los los registros del administrador y los operadores	RA24	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a errores del administrador	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[E.17] Vulnerabilidades de los programas (software)	Pruebas al software inexistentes o insuficientes Falta de documentación	RA25	Riesgo asociado a los fallos o errores en las aplicaciones empresariales	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
		Configuración incorrecta de parámetros		debido a vulnerabilidades en los programas						
		Mala administración de claves								
		Falta de control de cambios eficaz								
	[E.18] Errores de mantenimiento / Actualización de programas (software)	Pruebas al software inexistentes o insuficientes	RA26	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a errores de mantenimiento o en la actualización del código	1	RARO	3	MODERADO	3	RIESGO BAJO
		Errores conocidos en el software								
		Interfaz de usuario complicada								
		Falta de documentación								
		Configuración incorrecta de parámetros								
	[A.1] Manipulación de la configuración	Falta de control de cambios de configuración	RA27	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a algún error de configuración	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
		Configuración incorrecta de parámetros								
		Uso incorrecto de software y hardware								
	[A.4] Re-Encadenamiento de mensajes	Falta de mecanismos de identificación y autentificación de usuarios	RA28	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a al envío de información a un destino incorrecto a través de los sistemas o la red	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Arquitectura de red insegura								
		Ausencia de personal								
	[A.11] Denegación de servicio	Uso incorrecto de software y hardware	RA29	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido a la denegación de algún servicio	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
		Configuración incorrecta de parámetros								
		Falta de un control eficiente del cambio de configuración								
	[A.15] Abuso de privilegios de acceso	Capacitación en seguridad insuficiente	RA30	Riesgo asociado a los fallos o errores en las aplicaciones empresariales debido al abuso de privilegios de acceso	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Falta de conciencia del personal								
		Mecanismos de monitoreo deficientes								
Software gubernamental	[I.4] Avería de origen físico y lógico	Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA31	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a defectos de origen físico o lógico durante su funcionamiento	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
		Uso incorrecto de software y hardware								
	[E.1] Errores de configuración	Falta de un control eficiente del cambio de configuración	RA32	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a la introducción de datos de configuración en forma errónea	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Configuración incorrecta de parámetros								
		Habilitación de servicios innnecesarios								
		Uso incorrecto de software y hardware								
	[E.3] Difusión de software dañino	Falta de conciencia del personal	RA33	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a la propagación de algún software dañino	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
		Descarga y uso incontrolado de software								
		Mecanismos de monitoreo deficientes								

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
		Falta de una política de uso de correo electrónico								
		Computadoras personales sin programas antivirus								
	[E.19] Errores del administrador	Uso incorrecto de software y hardware	RA34	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a errores del administrador	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Mecanismos de monitoreo deficientes								
		Capacitación en seguridad insuficiente								
		Ausencia de informes de fallas registradas en los los registros del administrador y los operadores								
	[E.17] Vulnerabilidades de los programas (software)	Pruebas al software inexistentes o insuficientes	RA35	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a vulnerabilidades en los programas	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Falta de documentación								
		Configuración incorrecta de parámetros								
		Mala administración de claves								
		Falta de control de cambios eficaz								
	[E.18] Errores de mantenimiento / Actualización de programas (software)	Pruebas al software inexistentes o insuficientes	RA36	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a errores de mantenimiento o en la actualización del código	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
		Errores conocidos en el software								
		Interfaz de usuario complicada								
		Falta de documentación								
		Configuración incorrecta de parámetros								
	[A.1] Manipulación de la configuración	Falta de control de cambios de configuración	RA37	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a algún error de configuración	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
		Configuración incorrecta de parámetros								
		Uso incorrecto de software y hardware								
	[A.4] Re-Encadenamiento de mensajes	Falta de mecanismos de identificación y autentificación de usuarios	RA38	Riesgo asociado a los fallos o errores enlos sistemas gubernamentales debido a al envío de información a un destino incorrecto a través de los sistemas o la red	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Arquitectura de red insegura								
		Ausencia de personal								
	[A.11] Denegación de servicio	Uso incorrecto de software y hardware	RA39	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido a la denegación de algún servicio	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
		Configuración incorrecta de parámetros								
		Falta de un control eficiente del cambio de configuración								
	[A.15] Abuso de privilegios de acceso	Capacitación en seguridad insuficiente	RA40	Riesgo asociado a los fallos o errores en los sistemas gubernamentales debido al abuso de privilegios de acceso	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Falta de conciencia del personal								
		Mecanismos de monitoreo deficientes								

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
Equipos de comunicación central	[I.3] Contaminación mecánica	Susceptibilidad a la humedad, al polvo y a la suciedad Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA41	Riesgo asociado a problemas en los equipos de comunicación central debido a la contaminación mecánica	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[I.5] Corte de suministro eléctrico	Red de energía eléctrica inestable Variaciones de voltaje	RA42	Riesgo asociado a problemas en los equipos de comunicación central debido fallas eléctricas	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
	[I.6] Condiciones inadecuadas de temperatura y humedad	Susceptibilidad a la humedad, al polvo y a la suciedad Variaciones de voltaje	RA43	Riesgo asociado a problemas en los equipos de comunicación central debido a fallas en la climatización	2	IMPROBABLE	3	MODERADO	6	RIESGO MODERADO
	[I.7] Fallo de servicios de comunicaciones	Falta de un control eficiente del cambio de configuración Arquitectura de red insegura Líneas de comunicación no protegidas Falta de una política de uso de correo electrónico	RA44	Riesgo asociado a problemas en los equipos de comunicación central debido fallos en los servicios de comunicación	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[E.4] Errores de Re-Encadenamiento de mensajes	Falta de mecanismos de identificación y autentificación de usuarios Arquitectura de red insegura Ausencia de personal	RA45	Riesgo asociado a problemas en los equipos de comunicación central debido envío incorrecto de la información a través de la red	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[A.1] Manipulación de la configuración	Falta de control de cambios de configuración Configuración incorrecta de parámetros Uso incorrecto de software y hardware	RA46	Riesgo asociado a problemas en los equipos de comunicación central debido a errores en la configuración de algún activo	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
	[A.11] Denegación de servicio	Uso incorrecto de software y hardware Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración	RA47	Riesgo asociado a problemas en los equipos de comunicación central debido a la denegación de algún servicio	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[A.12] Robo	Acceso físico no autorizado Acceso no autorizado a la infraestructura informática Falta de políticas de seguridad Falta de Planes de continuidad	RA48	Riesgo asociado a problemas en los equipos de comunicación central debido a la sustracción de algún equipo	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
Red física (cableado)	[I.3] Contaminación mecánica	Susceptibilidad a la humedad, al polvo y a la suciedad Mantenimiento insuficiente/Instalación fallida de medios de mantenimiento	RA49	Riesgo asociado a problemas en las redes y comunicaciones debido a la contaminación mecánica	5	CASI SEGURO	4	SIGNIFICATIVO	20	RIESGO EXTREMO

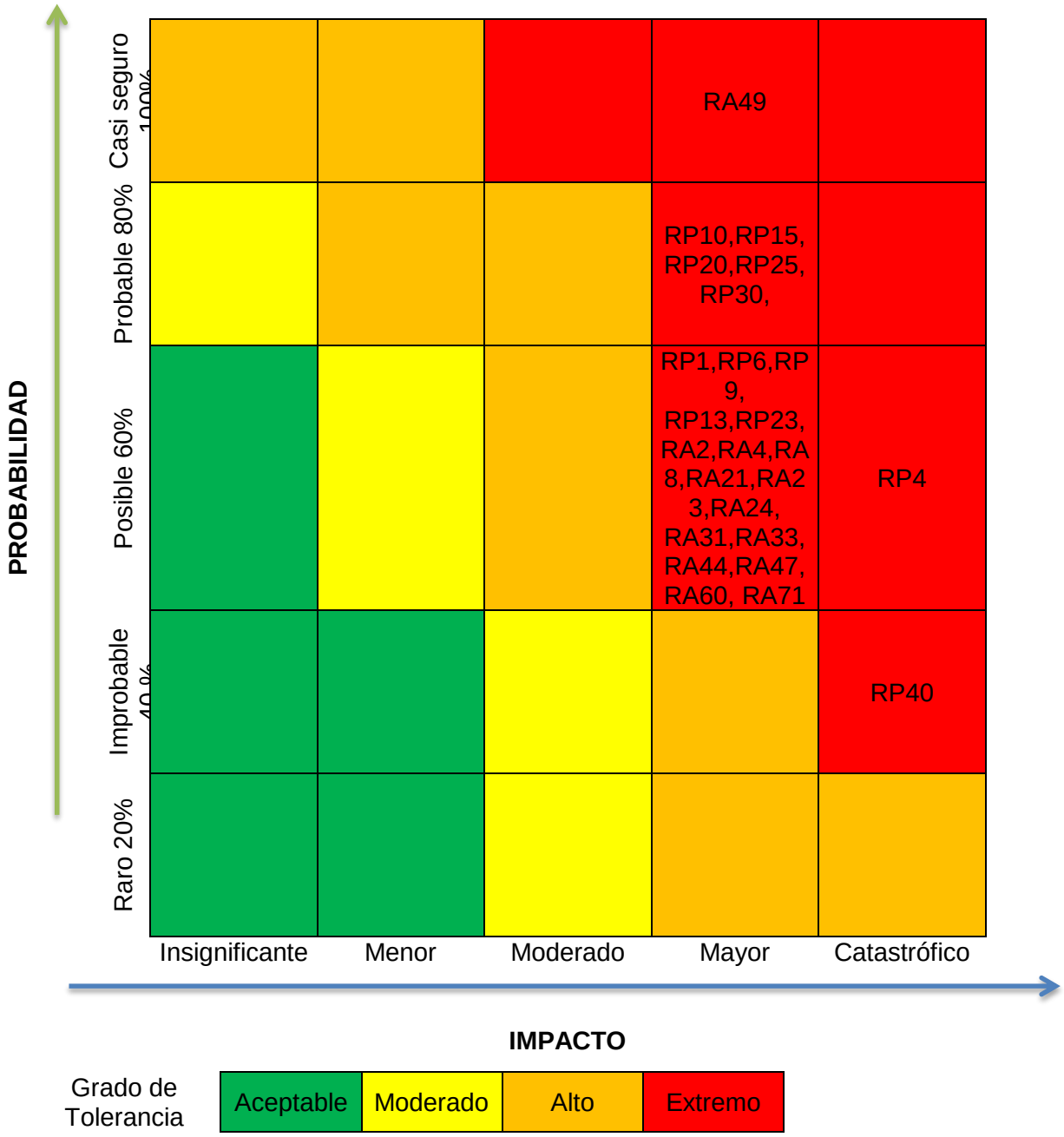
Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[I.6] Condiciones inadecuadas de temperatura y humedad	Susceptibilidad a la humedad, al polvo y a la suciedad Variaciones de voltaje	RA50	Riesgo asociado a problemas enlas redes y comunicaciones debido a fallas en la climatización	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[I.7] Fallo de servicios de comunicaciones	Falta de un control eficiente del cambio de configuración Arquitectura de red insegura Líneas de comunicación no protegidas Falta de una política de uso de correo electrónico	RA51	Riesgo asociado a problemas en las redes y comunicaciones debido fallos en los servicios de comunicación	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
	[E.4] Errores de Re-Encadenamiento de mensajes	Falta de mecanismos de identificación y autentificación de usuarios Arquitectura de red insegura Ausencia de personal	RA52	Riesgo asociado a problemas en las redes y comunicaciones debido envío incorrecto de la información a través de la red	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[E.6] Escapes de información	Habilitación de servicios innnecesarios Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	RA53	Riesgo asociado a problemas en las redes y comunicaciones debido salida de información no autorizada	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[A.1] Manipulación de la configuración	Falta de control de cambios de configuración Configuración incorrecta de parámetros Uso incorrecto de software y hardware	RA54	Riesgo asociado a problemas en las redes y comunicaciones debido a errores en la configuración de algún activo	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
	[A.2] Uso no previsto	Uso incorrecto de software y hardware Falta de conciencia del personal Capacitación en seguridad insuficiente	RA55	Riesgo asociado a problemas en las redes y comunicaciones debido a la utilización de recursos del sistema para fines no previstos	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
	[A.11] Denegación de servicio	Uso incorrecto de software y hardware Configuración incorrecta de parámetros Falta de un control eficiente del cambio de configuración	RA56	Riesgo asociado a problemas en las redes y comunicaciones debido a la denegación de algún servicio	4	PROBABLE	3	MODERADO	12	RIESGO EXTREMO
	[A.12] Robo	Acceso físico no autorizado Acceso no autorizado a la infraestructura informática Falta de políticas de seguridad Falta de Planes de continuidad	RA57	Riesgo asociado a problemas en las redes y comunicaciones debido a la sustracción de algún equipo	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
Responsable de tomar decisiones	[E.2] Deficiencias en la organización	Falta de revisiones regulares de la gestión Falta de asignación apropiada de responsabilidades de seguridad de la información	RA58	Riesgo asociado a la ausencia o indisponibilidad del responsable en las tomas de decisiones en seguridad	4	PROBABLE	3	MODERADO	12	RIESGO EXTREMO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
		Falta de procedimientos para reportar debilidades en la seguridad de la información		debido a deficiencias de coordinación, omisiones, acciones mal realizadas, etc.						
		Falta de Planes de continuidad								
		Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información								
		Falta de autorización de acceso a las instalaciones del procesamiento de la información								
	[E.6] Escapes de información	Falta de cuidado al descartarlo	RA59	Riesgo asociado a la ausencia o indisponibilidad del responsable en las tomas de decisiones en seguridad debido a salida de información no autorizada	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Copia no controlada								
		Habilitación de servicios innnecesarios								
		Falta de copias de respaldo								
		Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería								
	[E.13] Indisponibilidad del personal	Ausencia de personal	RA60	Riesgo asociado a la ausencia o indisponibilidad del responsable en las tomas de decisiones en seguridad debido a la ausencia en su puesto de trabajo	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
		Falta de Planes de continuidad								
	[A.6] Interceptación de información (escucha)	Líneas de comunicación no protegidas	RA61	Riesgo asociado a la ausencia o indisponibilidad del responsable en las tomas de decisiones en seguridad debido a interceptación de la información	2	IMPROBABLE	4	SIGNIFICATIVO	8	RIESGO ALTO
		Almacenamiento no protegido								
		Falta de cuidado al descartarlo								
		Copia no controlada								
		Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería								
		Arquitectura de red insegura								
	[A.21] Ingeniería social	Capacitación en seguridad insuficiente	RA62	Riesgo asociado a la ausencia o indisponibilidad del responsable en las tomas de decisiones en seguridad debido al abuso de la buena fe que tiene para realizar actividades con terceros	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
		Falta de conciencia del personal								
		Mecanismos de monitoreo deficientes								
Personal		Falta de revisiones regulares de la gestión	RA63		4	PROBABLE	3	MODERADO	12	RIESGO EXTREMO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[E.2] Deficiencias en la organización	Falta de asignación apropiada de responsabilidades de seguridad de la información		Riesgo asociado a la ausencia o indisponibilidad del personal de operaciones y mantenimiento debido a deficiencias de coordinación, omisiones, acciones mal realizadas, etc.						
		Falta de procedimientos para reportar debilidades en la seguridad de la información								
		Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información								
		Falta de autorización de acceso a las instalaciones del procesamiento de la información								
	[E.6] Escapes de información	Falta de cuidado al descartarlo	RA64	Riesgo asociado a la ausencia o indisponibilidad del personal de operaciones y mantenimiento debido a salida de información no autorizada	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
		Copia no controlada								
		Habilitación de servicios innnecesarios								
		Falta de copias de respaldo								
		Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería								
	[E.13] Indisponibilidad del personal	Ausencia de personal	RA65	Riesgo asociado a la ausencia o indisponibilidad del personal de operaciones y mantenimiento debido a la ausencia en su puesto de trabajo	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
		Falta de Planes de continuidad								
	[E.15] Errores del administrador	Capacitación en seguridad insuficiente	RA66	Riesgo asociado a la ausencia o indisponibilidad del personal de operaciones y mantenimiento en seguridad debido a la ausencia en su puesto de trabajo	3	POSIBLE	3	MODERADO	9	RIESGO ALTO
		Ausencia de informes de fallas registradas en los los registros del administrador y los operadores								
		Falta de procedimientos de control de cambios								
		Mecanismos de monitoreo deficientes								
	[A.6] Interceptación de información (escucha)	Líneas de comunicación no protegidas	RA67	Riesgo asociado a la ausencia o indisponibilidad del personal de operaciones y mantenimiento debido a equivocaciones en las instalaciones y las operaciones	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO
		Almacenamiento no protegido								
		Falta de cuidado al descartarlo								
		Copia no controlada								
		Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería								
		Arquitectura de red insegura								

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[A.21] Ingeniería social	Capacitación en seguridad insuficiente Falta de conciencia del personal Mecanismos de monitoreo deficientes	RA68	Riesgo asociado a la ausencia o indisponibilidad del personal de operaciones y mantenimiento debido al abuso de la buena fe que tiene para realizar actividades con terceros	1	RARO	2	MENOR	2	RIESGO BAJO
Sala de servidores	[N.1] Fuego	Susceptibilidad a variaciones de temperatura Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas Falta de Planes de continuidad Instalaciones sin extintores	RA69	Riesgo asociado a daño en la sala de servidores debido a un incendio	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[N.2] Daños por agua	Falta de Planes de continuidad Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas Ubicaciones en áreas susceptibles a inundaciones	RA70	Riesgo asociado a daño en la sala de servidores debido a perjuicios ocasionados por egua	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[A.16] Acceso no autorizado	Asignación equivocada de derechos de acceso Capacitación en seguridad insuficiente Falta de conciencia del personal Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas	RA71	Riesgo asociado a daño en la sala de servidores debido a algún acceso no autorizado	3	POSIBLE	4	SIGNIFICATIVO	12	RIESGO EXTREMO
	[A.20] Ataque destructivo	Almacenamiento no protegido Falta de protección física del edificio, puertas y ventanas Mecanismos de monitoreo deficientes Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas	RA72	Riesgo asociado a daño en la sala de servidores debido al ataque destructivo propio del personal interno o externos al CGT	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
Servicios esenciales	[N.1] Fuego	Susceptibilidad a variaciones de temperatura Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas Falta de Planes de continuidad Instalaciones sin extintores	RA73	Riesgo asociado a daño en los servicios esenciales debido a un incendio	1	RARO	5	CATASTROFICO	5	RIESGO BAJO

Identificación del riesgo					Evaluación del riesgo					
Activo	Amenazas potenciales	Vulnerabilidades encontradas	Formulación del riesgo		Probabilidad		Impacto		Nivel de riesgo	
			Id Riesgo	Identificación	Calif.	Significado	Calif.	Significado	Calif.	Significado
	[N.2] Daños por agua	Falta de Planes de continuidad Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas Ubicaciones en áreas susceptibles a inundaciones	RA74	Riesgo asociado a daño en los servicios esenciales debido a perjuicios ocasionados por egua	1	RARO	5	CATASTROFICO	5	RIESGO BAJO
	[A.16] Acceso no autorizado	Asignación equivocada de derechos de acceso Capacitación en seguridad insuficiente Falta de conciencia del personal Uso inadecuado y negligente del control de acceso físico a edificios y habitaciones protegidas	RA75	Riesgo asociado a daño en los servicios esenciales debido a algún acceso no autorizado	3	POSIBLE	1	INSIGNIFICANTE	3	RIESGO BAJO
	[A.20] Ataque destructivo	Almacenamiento no protegido Falta de protección física del edificio, puertas y ventanas Mecanismos de monitoreo deficientes Falta de Planes de continuidad	RA76	Riesgo asociado a daño en los servicios esenciales debido al ataque destructivo propio del personal interno o externos al CGT	1	RARO	4	SIGNIFICATIVO	4	RIESGO BAJO



Grado de Tolerancia	Aceptable	Moderado	Alto	Extremo

Figura N° 21. Identificación de los riesgos no tolerables
Fuente: Desarrollo Propio

4.5. Identificación y evaluación de las opciones para el tratamiento del riesgo en seguridad de la información

Con la lista de riesgos priorizada de acuerdo con criterios de evaluación del riesgo en relación con los escenarios de incidentes que llevan a esos riesgos se debe seleccionar controles para reducir, retener, evitar o transferir los riesgos y un plan del tratamiento del riesgo definido.

La Gerencia CGT cuenta con varias opciones para el tratamiento del riesgo que no se excluyen mutuamente. El objetivo es que la CGT se beneficie sustancialmente por una combinación de opciones como la reducción de la posibilidad de riesgos, la reducción de sus consecuencias, y la transferencia o retención de cualquier riesgo residual.

4.5.1. Plan de tratamiento de riesgos

Con el propósito de alcanzar los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información, se establecen los siguientes controles de seguridad ya seleccionados basados en el Anexo A de la norma NTP ISO/IEC 27001:2014.

A continuación se mostraran los riesgos extremos, con la decisión de aceptación (Estrategia), así como el propietario de dicho riesgo, teniendo como fin responsabilizarlo por monitorear el riesgo identificado y gestionar el plan de tratamiento, independiente de que él sea el responsable de implementar las acciones registradas en dicho plan.

Tabla N° 54. Plan de tratamiento de riesgos en base a la norma NTP ISO/IEC 27001:2014

Id riesgo	Formulación del riesgo	Nivel de riesgo	Propietario del riesgo	Control implementado	Estrategia
RP1	Riesgo asociado a interrupciones en el proceso de Gestión administrativa del CGT originado por fallos en los equipos y/o fallos en los programas.	RIESGO EXTREMO	Oficina General de Administración	A.11.2.4. Mantenimiento de equipos A.12.6.1 Gestión de vulnerabilidades técnicas	MITIGAR
RP4	Riesgo asociado a interrupciones en el proceso de Gestión administrativa debido a la saturación de los sistemas informáticos.	RIESGO EXTREMO	Oficina General de Administración	A.12.1.3 Gestión de la capacidad	MITIGAR
RP6	Riesgo asociado a interrupciones en el proceso de Gestión Tributaria originado por fallos en los equipos y/o fallos en los programas.	RIESGO EXTREMO	División de recaudación y control de deuda	A.11.2.4. Mantenimiento de equipos A.12.6.1 Gestión de vulnerabilidades técnicas	MITIGAR
RP9	Riesgo asociado a interrupciones en el proceso de Gestión Tributaria debido a la saturación de los sistemas informáticos.	RIESGO EXTREMO	División de recaudación y control de deuda	A.12.1.3 Gestión de la capacidad	MITIGAR
RP10	Riesgo asociado a interrupciones en el proceso de Gestión Tributaria debido a las equivocaciones de los usuarios cuando usan los equipos o sistemas informáticos.	RIESGO EXTREMO	División de recaudación y control de deuda	A.12.4.1 Registro de eventos	MITIGAR
RP13	Riesgo asociado a la pérdida o daño de la información contenida en las bases de datos del CGT debido a la introducción incorrecta de información.	RIESGO EXTREMO	Oficina de TI	A.7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	TRANSFERIR
RP15	Riesgo asociado a la pérdida o daño de la información contenida en las bases de datos del CGT a causa de las equivocaciones de los	RIESGO EXTREMO	Oficina de TI	A.12.4.1 Registro de eventos	MITIGAR

Id riesgo	Formulación del riesgo	Nivel de riesgo	Propietario del riesgo	Control implementado	Estrategia
	usuarios cuando usan los equipos o sistemas informáticos.				
RP20	Riesgo asociado a la pérdida o daño de la información contenida en las bases de datos del CGT a causa de algún acceso no autorizado.	RIESGO EXTREMO	Oficina de TI	A.9.1.1 Política de control de acceso A.9.2.1 Registro y baja de usuarios A.12.4.2 Protección de información de registros. A.18.1.3 Protección de registros	MITIGAR
RP23	Riesgo asociado a la pérdida o daño de la información contenida en sistemas gubernamentales externos debido a la introducción incorrecta de información.	RIESGO EXTREMO	Oficina de TI	A.7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	TRANSFERIR
RP25	Riesgo asociado a la pérdida o daño de la información contenida en sistemas gubernamentales externos a causa de las equivocaciones de los usuarios cuando usan los equipos o sistemas informáticos.	RIESGO EXTREMO	Oficina de TI	A.12.4.1 Registro de eventos	MITIGAR
RP30	Riesgo asociado a la pérdida o daño de la información contenida en sistemas gubernamentales externos a causa de algún acceso no autorizado.	RIESGO EXTREMO	Oficina de TI	A.9.1.1 Política de control de acceso A.9.2.1 Registro y baja de usuarios A.12.4.2 Protección de información de registros. A.18.1.3 Protección de registros	MITIGAR
RP40	Riesgo asociado a la pérdida o daño de la información confidencial del CGT a causa de algún acceso no autorizado.	RIESGO EXTREMO	Oficina de Control Interno	A.9.1.1 Política de control de acceso A. 9.2.4 Gestión de información de autentificación secreta de usuarios A.9.3.1 Uso de información de autentificación secreta A.12.4.2 Protección de información de registros. A.18.1.3 Protección de registros	MITIGAR
RA2	Riesgo asociado a fallos en los servidores debido a alguna avería física o lógica que los afecte.	RIESGO EXTREMO	Oficina de TI	A.11.2.4. Mantenimiento de equipos A.12.6.1 Gestión de vulnerabilidades técnicas	MITIGAR
RA4	Riesgo asociado a fallos en los servidores debido a errores de configuración.	RIESGO EXTREMO	Oficina de TI	A.12.4.3 Registros del administrador y del operador	MITIGAR
RA8	Riesgo asociado a fallos en los servidores debido a errores de mantenimiento o actualización de equipos.	RIESGO EXTREMO	Oficina de TI	A.11.2.4 Mantenimiento de equipos A.12.6.1 Gestión de vulnerabilidades técnicas	MITIGAR
RA21	Riesgo asociado a fallos o errores en las aplicaciones empresariales debido a un defecto de origen físico o lógico durante su funcionamiento.	RIESGO EXTREMO	Jefes de las áreas orgánicas y funcionales del CGT	A.11.2.4. Mantenimiento de equipos A.12.6.1 Gestión de vulnerabilidades técnicas	MITIGAR

Id riesgo	Formulación del riesgo	Nivel de riesgo	Propietario del riesgo	Control implementado	Estrategia
RA23	Riesgo asociado a fallos o errores en las aplicaciones empresariales debido a la propagación de algún software dañino.	RIESGO EXTREMO	Jefes de las áreas orgánicas y funcionales del CGT	A.12.2.1 Controles contra códigos maliciosos A.12.6.2 Restricciones sobre la instalación de software	MITIGAR
RA24	Riesgo asociado a fallos o errores en las aplicaciones empresariales del CGT debido a errores del administrador.	RIESGO EXTREMO	Jefes de las áreas orgánicas y funcionales del CGT	A.12.4.3 Registros del administrador y del operador A.14.2.2 Procedimiento de control de cambio sistema A.14.2.4 Restricciones sobre cambios a los paquetes de software	MITIGAR
RA31	Riesgo asociado a fallos o errores en los sistemas gubernamentales debido a un defecto de origen físico o lógico durante su funcionamiento.	RIESGO EXTREMO	Jefes de las áreas orgánicas y funcionales del CGT	A.11.2.4. Mantenimiento de equipos A.12.6.1 Gestión de vulnerabilidades técnicas	MITIGAR
RA33	Riesgo asociado a fallos o errores en los sistemas gubernamentales del CGT debido a la propagación de algún software dañino.	RIESGO EXTREMO	Jefes de las áreas orgánicas y funcionales del CGT	A.12.2.1 Controles contra códigos maliciosos A.12.6.2 Restricciones sobre la instalación de SW.	MITIGAR
RA44	Riesgo asociado a problemas en los equipos de comunicación central del CGT debido a fallos en los servicios de comunicación.	RIESGO EXTREMO	Oficina de TI	A.11.2.3 Seguridad del cableado A.13.1.1 Controles de la red A.13.1.2 Seguridad de servicios de red	MITIGAR
RA47	Riesgo asociado a problemas en los equipos de comunicación central del CGT a causa de alguna denegación de servicios	RIESGO EXTREMO	Oficina de TI	A.9.1.2 Acceso a redes y servicios de red A.12.1.3 Gestión de la capacidad	MITIGAR
RA49	Riesgo asociado a problemas en las redes y comunicaciones del CGT debido a la contaminación mecánica.	RIESGO EXTREMO	Oficina de TI	A.11.2.4. Mantenimiento de equipos	MITIGAR
RA71	Riesgo asociado a daño en la sala de servidores del CGT debido algún acceso no autorizado.	RIESGO EXTREMO	Oficina de TI	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de ingreso físico A.11.1.3 Asegurar oficinas, áreas e instalaciones	TRANSFERIR

La presente tesis no determinara los riesgos residuales, sin embargo se propone que el Área de TI haga la evaluación del plan de tratamiento para ver los controles planteados y con ellos obtener el riesgo residual, para luego realizar una actualización o reiteración de la evaluación del riesgo, tomando en cuenta los efectos esperados del tratamiento propuesto del riesgo. Además si el riesgo residual todavía no cumple con los criterios de aceptación del riesgo del CGT, puede ser necesaria una nueva iteración del tratamiento del riesgo antes de proceder a la aceptación del riesgo.

4.5.2. Aceptación del riesgo en seguridad de la información

Los planes de tratamiento del riesgo deben describir cómo se deben tratar los riesgos evaluados para satisfacer los criterios de aceptación del riesgo. Es importante que la Gerencia CGT revise y aprueben los planes de tratamiento del riesgo propuestos y los riesgos residuales resultantes y registrar cualquier condición que se asocie con dicha aprobación.

Los criterios de aceptación del riesgo pueden ser más complejos que simplemente determinar si un riesgo residual cae o no por encima o por debajo de un umbral específico.

En algunos casos el nivel de riesgo residual puede no cumplir con los criterios de aceptación del riesgo porque los criterios que se están aplicando no toman en cuenta las circunstancias prevalecientes.

4.5.3. Comunicación del riesgo en seguridad de la información

La comunicación del riesgo es una actividad para lograr acuerdos sobre cómo manejar los riesgos intercambiando y/o compartiendo información sobre el riesgo entre quienes toman las decisiones y otros interesados. La información incluye, pero no se limita a, la existencia, naturaleza, forma, posibilidad, gravedad, tratamiento y aceptabilidad de los riesgos.

La comunicación eficaz entre los interesados es importante ya que esto puede tener un impacto significativo en las decisiones que se deben tomar. La comunicación asegurará que los responsables de implementar la gestión del riesgo y aquellos que tienen intereses particulares comprendan la base sobre la cual se toman las decisiones y las acciones particulares que se requieren. La comunicación es bi-direccional.

El riesgo para operaciones normales, así como las situaciones de emergencia serán comunicados haciendo uso de los formatos establecidos lo que permitirá que el Comité de Seguridad de la Información y la Gerencia CGT debatan los riesgos, su priorización y su tratamiento apropiado y aceptación.

Es importante cooperar con el Comité de Seguridad de la Información para coordinar todas las tareas relacionadas con la comunicación del riesgo. Esto es crucial en el caso de acciones de comunicación de la crisis.

4.5.4. Enunciado de aplicabilidad

Este documento, requerido por la Norma Técnica Peruana ISO/IEC 27001:2014, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados.

En esta herramienta se ha registrado todo lo que se ha realizado y se va a realizar en el futuro inmediato para que la seguridad de la información del CGT llegue al nivel que se haya estimado apropiado para sus necesidades y recursos.

Razón por la cual la declaración de aplicabilidad debe incluir los controles apropiados en el punto anterior.

Para cada uno de los controles debe reflejarse en este documento:

a. Si está implantado actualmente en la organización, con una breve descripción de por qué se aplica.

b. Si se va a implantar, es decir, si es uno de los controles escogidos para mitigar el riesgo, junto con las razones para haberlo seleccionado.

c. Si no se va a implantar, y entonces hay que exponer los motivos que han llevado a esta decisión. Las exclusiones deben justificarse adecuadamente.

El principal objetivo de este ítem es que, al tener que repasar todos y cada uno de los controles, se hace una comprobación de que no se ha pasado por alto ningún control por error o descuido, que podría ser útil o necesario para la gestión de la seguridad de la información.

Esta herramienta es un registro de los resultados finales del SGSI, ya que concreta de manera clara y directa en qué consiste el sistema gestión de seguridad de la información.

Se utilizará un código de colores que indica el estado en que se encuentra el control para una mejor gestión de su estado (rojo: necesario pero no se ha iniciado su implantación, amarillo: necesario y en proceso de implantación, verde: implantado).

Tabla N° 55. Revisión de la aplicabilidad de los controles

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
A.5.1 Dirección de la gerencia para la seguridad de la información			
Objetivo de control: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.			
A.5.1.1	Políticas para la seguridad de la información	Control Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.	Formular las pautas que tanto la Gerencia General y los empleados deban de cumplir para la implementación del Sistema de Gestión de Seguridad de la Información.
A.5.1.2	Revisión de la política de seguridad de la información	Control Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua.	Monitoreo, seguimiento y mejoramiento del Sistema de Gestión de Seguridad de la Información.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1 Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Control Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.	Definir la estructura que soportará el sistema de Gestión de Seguridad de la información. Este control esta descrito en la Política General de Seguridad de la Información.
A.6.1.2	Segregación de funciones	Control Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.	Definir la estructura que soportará el sistema de Gestión de Seguridad de la información. Este control esta descrito en la Política General de Seguridad de la Información.
A.6.1.3	Contacto con autoridades	Control Contactos apropiados con autoridades relevantes deben ser mantenidos.	No es prioridad para su implantación.
A.6.1.4	Contacto con grupos especiales de interés	Control Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos.	No es prioridad para su implantación.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.	No es prioridad para su implantación.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.7.1 Antes del empleo			
Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.			
A.7.1.1	Selección	Control Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	Apoyar en la gestión de personal. Es el área de Recursos humanos que realiza el proceso de selección y reclutamiento, y como parte de este proceso se revisan los antecedentes penales y policiales de cada uno de los candidatos a un puesto laboral dentro del CGT.
A.7.1.2	Términos y condiciones de empleo	Control Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	Apoyar en la gestión de personal
A.7.2 Durante el empleo			
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.			
A.7.2.1	Responsabilidades de la gerencia	Control La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	Apoyar en la gestión de personal
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	Control Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Apoyar en la gestión de personal
A.7.2.3	Proceso disciplinario	Control Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.	Apoyar en la gestión de personal

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.7.3 Terminación o cambio del empleo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.			
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	Control Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.	Apoyar en la gestión de personal
A.8 GESTIÓN DE ACTIVOS			
A.8.1 Responsabilidad por los activo			
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.			
A.8.1.1	Inventario de activos	Control Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.	Identificación de Activos.
A.8.1.2	Propiedad de los activos	Control Los activos mantenidos en el inventario deben ser propios.	Identificación de propietario de los activos.
A.8.1.3	Uso aceptable de los activos	Control Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.	No es prioridad para su implantación.
A.8.1.4	Retorno de activos	Control Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	No es prioridad para su implantación.
A.8.2 Clasificación de la información			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización			
A.8.2.1	Clasificación de la información	Control La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	Formulación de los lineamientos para la clasificación de la información. Este control esta descrito en la Política General de Seguridad de la Información.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.8.2.2	Etiquetado de la información	Control Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.	No es prioridad para su implantación.
A.8.2.3	Manejo de activos	Control Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	No es prioridad para su implantación.
A.8.3 Manejo de los medios			
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.			
A.8.3.1	Gestión de medios removibles	Control Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	No es prioridad para su implantación.
A.8.3.2	Disposición de medios	Control Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.	No es prioridad para su implantación.
A.8.3.3	Transferencia de medios físicos	Control Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.	No es prioridad para su implantación.
A.9 CONTROL DE ACCESO			
A.9.1 Requisitos de la empresa para el control de acceso			
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información. Limitar el acceso a la información y a las instalaciones de procesamiento de la información.			
A.9.1.1	Política de control de acceso	Control Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Gestionar el control de accesos a la información.
A.9.1.2	Acceso a redes y servicios de red	Control Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	Gestionar el control de accesos.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.9.2 Gestión de acceso de usuario			
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.			
A.9.2.1	Registro y baja de usuarios	Control Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.	Gestionar el control de accesos. Este control esta descrito en la Política General de Seguridad de la Información, sin embargo aún no se ha iniciado su implantación.
A.9.2.2	Aprovisionamiento de acceso a usuario	Control Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	No es prioridad para su implantación.
A.9.2.3	Gestión de derechos de acceso privilegiados	Control La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.9.2.4	Gestión de información de autentificación secreta de usuarios	Control La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.	Gestionar el control de accesos.
A.9.2.5	Revisión de derechos de acceso de usuarios	Control Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.9.2.6	Remoción o ajuste de derechos de acceso	Control Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.	No es prioridad para su implantación.
A.9.3 Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.			
A.9.3.1	Uso de información de autentificación secreta	Control Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.	Gestionar el control de accesos.
A.9.4 Control de acceso a sistema y aplicación			
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.9.4.1	Restricción de acceso a la información	Control El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	No es prioridad para su implantación.
A.9.4.2	Procedimientos de ingreso seguro	Control Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.	No es prioridad para su implantación.
A.9.4.3	Sistema de gestión de contraseñas	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	No es prioridad para su implantación.
A.9.4.4	Uso de programas utilitarios privilegiados	Control El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.	No es prioridad para su implantación.
A.9.4.5	Control de acceso al código fuente de los programas	Control El acceso al código fuente de los programas debe ser restringido.	No es prioridad para su implantación.
A.11. SEGURIDAD FÍSICA Y AMBIENTAL			
A.11.1 Áreas seguras			
Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.			
A.11.1.1	Perímetro de seguridad física	Control Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.	Administrar la protección física y ambiental de los activos seleccionados.
A.11.1.2	Controles de ingreso físico	Control Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	Administrar la protección física y ambiental de los activos seleccionados. Este control esta descrito en la Política General de Seguridad de la Información, sin embargo no se ha iniciado su implantación.
A.11.1.3	Asegurar oficinas, áreas e instalaciones	Control Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.	Administrar la protección física y ambiental de los activos seleccionados.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.11.1.4	Protección contra amenazas externas y ambientales	Control Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	No es prioridad para su implantación.
A.11.1.5	Trabajo en áreas seguras	Control Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	No es prioridad para su implantación.
A.11.2 Equipos			
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.			
A.11.2.1	Emplazamiento y protección de los equipos	Control Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.11.2.2	Servicios de suministro	Control Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.11.2.3	Seguridad del cableado	Control El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.	Proteger la información. Este control esta descrito en la Política General de Seguridad de la Información y se encuentra en proceso de implantación.
A.11.2.4	Mantenimiento de equipos	Control Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	Asegurar la disponibilidad e integridad de los equipos. Este control esta descrito en la Política General de Seguridad de la Información y se encuentra en proceso de implantación.
A.11.2.5	Remoción de activos	Control Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.	Seguridad de los activos.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.	No es prioridad para su implantación.
A.11.2.7	Disposición o reutilización segura de equipos	Control Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.	Asegurar la confidencialidad de los equipos que contengan medios de almacenamiento.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.11.2.8	Equipos de usuario desatendidos	Control Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.12 SEGURIDAD DE LAS OPERACIONES			
A.12.1 Procedimientos y responsabilidades operativas			
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.			
A.12.1.1	Procedimientos operativos documentados	Control Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.	No es prioridad para su implantación.
A.12.1.2	Gestión del cambio	Control Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.12.1.3	Gestión de la capacidad	Control El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Planificar el sistema
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Control Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.12.2 Protección contra códigos maliciosos			
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.			
A.12.2.1	Controles contra códigos maliciosos	Control Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.	Mitigar el riesgo generado por software malicioso. Este control esta descrito en la Política General de Seguridad de la Información y se encuentra en proceso de implantación.
A.12.3 Respaldo			
Objetivo: Proteger contra la pérdida de datos			

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.12.3.1	Respaldo de la información	Control Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.12.4 Registros y monitoreo			
Objetivo: Registrar eventos y generar evidencia			
A.12.4.1	Registro de eventos	Control Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.	Registrar eventos y generar evidencia de las actividades de los usuarios.
A.12.4.2	Protección de la información del registro	Control Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	Proteger los medios de registro y la información de los registros
A.12.4.3	Registros del administrador y operador	Control Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.	Registrar eventos y generar evidencia de las actividades del administrador y del operador del sistema.
A.12.4.4	Sincronización de reloj	Control Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben esta sincronizados a una fuente de tiempo de referencia única.	No es prioridad para su implantación.
A.12.5 Control del software operacional			
Objetivo: Asegurar la integridad de los sistemas operacionales			
A.12.5.1	Instalación de software en sistemas operacionales	Control Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.	No es prioridad para su implantación.
A.12.6 Gestión de vulnerabilidad técnica			
Objetivo: Prevenir la explotación de vulnerabilidades técnicas			
A.12.6.1	Gestión de vulnerabilidades técnicas	Control Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	Gestionar la aplicación de recomendaciones para evitar la que una amenaza explote una vulnerabilidad.
A.12.6.2	Restricciones sobre la instalación de software	Control	Gestionar la instalación de software para evitar la que una amenaza explote una vulnerabilidad.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
		Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	
A.12.7 Consideraciones para la auditoría de los sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.			
A.12.7.1	Controles de auditoría de sistemas de información	Control Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.	No es prioridad para su implantación.
A.13 SEGURIDAD DE LAS COMUNICACIONES			
A.13.1 Gestión de seguridad de la red			
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.			
A.13.1.1	Controles de la red	Control Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	Gestionar la seguridad de la red
A.13.1.2	Seguridad de servicios de red	Control Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	Gestionar la seguridad de la red. Este control esta descrito en la Política General de Seguridad de la Información, sin embargo no se ha iniciado su implantación.
A.13.1.3	Segregación en redes	Control Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.	No es prioridad para su implantación.
A.13.2 Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			
A.13.2.1	Políticas y procedimientos de transferencia de la información	Control Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	No es prioridad para su implantación.
A.13.2.2	Acuerdo sobre transferencia de información	Control Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	No es prioridad para su implantación.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.13.2.3	Mensajes electrónicos	Control La información involucrada en mensajería electrónica debe ser protegido apropiadamente.	No es prioridad para su implantación.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Control Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.	Asegurar la confidencialidad de la información.
A.14 Adquisición, desarrollo y mantenimiento de sistemas			
A.14.1 Requisitos de seguridad de los sistemas de información			
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes.	No es prioridad para su implantación.
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	Control La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegido de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.	No es prioridad para su implantación.
A.14.1.3	Protección de transacciones en servicios de aplicación	Control La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.	No es prioridad para su implantación.
A.14.2 Seguridad en los procesos de desarrollo y soporte			
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.1	Política de desarrollo seguro	Control Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.	No es prioridad para su implantación.
A.14.2.2	Procedimientos de control de cambio del sistema	Control Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.	Gestionar los cambios a los sistemas dentro del ciclo de vida del desarrollo.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Control Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.	No es prioridad para su implantación.
A.14.2.4	Restricciones sobre cambios a los paquetes de software	Control Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.	Gestionar los cambios a los paquetes de software.
A.14.2.5	Principios de ingeniería de sistemas seguros	Control Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.	No es prioridad para su implantación.
A.14.2.6	Ambiente de desarrollo seguro	Control Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.	No es prioridad para su implantación.
A.14.2.7	Desarrollo contratado externamente	Control La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.	No es prioridad para su implantación.
A.14.2.8	Pruebas de seguridad del sistema	Control Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.	No es prioridad para su implantación.
A.14.2.9	Pruebas de aceptación del sistema	Control Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.	No es prioridad para su implantación.
A.14.3 Datos de prueba			
Objetivo: Asegurar la protección de datos utilizados para las pruebas.			
A.14.3.1	Protección de datos de prueba	Control Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.			
A.16.1.1	Responsabilidades y procedimientos	Control Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	Establecer responsabilidades que gestione los incidentes de seguridad de la información. Forma parte de la Política para la gestión de Incidentes de la Seguridad de la Información.
A.16.1.2	Reporte de eventos de seguridad de la información	Control Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.	Reportar los eventos en la seguridad de la información. Forma parte de la Política para la gestión de Incidentes de la Seguridad de la Información.
A.16.1.3	Reporte de debilidades de seguridad de la información	Control Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	Reportar las debilidades en la seguridad de la información. Forma parte de la Política para la gestión de Incidentes de la Seguridad de la Información.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Control Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información.	Evaluar los eventos en la seguridad de la información. Forma parte de la Política para la gestión de Incidentes de la Seguridad de la Información. Forma parte de la Política para la gestión de Incidentes de la Seguridad de la Información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Gestionar los incidentes de seguridad de la información. Forma parte de la Política para la gestión de Incidentes de la Seguridad de la Información.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.	Fortalecer el proceso de mejora continua.
A.16.1.7	Recolección de evidencia	Control La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Apoyar procesos colaterales de la Seguridad de la Información.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
A.17.1 Continuidad de seguridad de la información			
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización			

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.17.1.1	Planificación de continuidad de seguridad de la información	Control La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	No es prioridad para su implantación.
A.17.1.2	Implementación de continuidad de seguridad de la información	Control La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	No es prioridad para su implantación.
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	Control La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	No es prioridad para su implantación.
A.17.2 Redundancias			
Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información			
A.17.2.1	Instalaciones de procesamiento de la información	Control Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	No es prioridad para su implantación.
A.18 CUMPLIMIENTO			
A.18.1 Cumplimiento con requisitos legales y contractuales			
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.			
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Control Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.	No es prioridad para su implantación.
A.18.1.2	Derechos de propiedad intelectual	Control Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.

OBJETIVOS DE CONTROL / CONTROLES			JUSTIFICACIÓN
A.18.1.3	Protección de registros	Control Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	Cumplir con los requerimientos legales y garantizar la continuidad de las operaciones de la entidad.
A.18.1.4	Privacidad y protección de datos personales.	Control La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.18.1.5	Regulación de controles criptográficos	Control Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.	No es prioridad para su implantación.
A.18.2 Revisiones de seguridad de la información			
Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.			
A.18.2.1	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.	No es prioridad para su implantación pero es necesario para cumplir con los estándares y políticas de seguridad de la información.
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Control Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	No es prioridad para su implantación, sin embargo parte de este control esta descrito en la Política General de Seguridad de la Información pero aún le falta implementarse.
A.18.2.3	Revisión del cumplimiento técnico	Control Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.	No es prioridad para su implantación pero es necesario para cumplir con los estándares y políticas de seguridad de la información.

4.5.5. Implementación y operación del sistema de gestión de seguridad de la información

A continuación se presenta un plan de tratamiento de riesgos para la realización de todo lo que se encuentra en proceso de implementación.

Tabla N° 56 Plan de implementación y operación del SGSI

Objetivos de control / controles		Fecha inicial	Fecha final	Responsable	Supervisor	Recursos
A.7.2.2	Implementar un programa de concientización en seguridad de la información a toda el CGT.			Personal que realiza labores de TIC	Gerencia CGT	Presentaciones grupales, manuales y folletos, cursos, coaching, teleconferencias, comunicados.
A.9.1.1	Desarrollar e implementar la política de control de acceso para limitar el acceso a la información.			Personal que realiza labores de TIC	Gerencia CGT	ISO/IEC 27002:2013
A.9.1.2	Desarrollar e implementar políticas y procedimientos al uso de redes y servicio de red.			Personal que realiza labores de TIC	Gerencia CGT	ISO/IEC 27002:2013
A.9.2.1	Implantar un proceso formal debidamente documentado de registro de usuario y de cancelación del registro para permitir la asignación de derechos de acceso.			Personal que realiza labores de TIC	Gerencia CGT	Computadora, bizagi
A.9.2.4	Establecer un proceso de gestión formal en la verificación de la identidad de un usuario antes de proporcionar información de autenticación secreta nueva, sustitutiva o temporal.			Personal que realiza labores de TIC, oficina de control interno	Gerencia CGT	Computadora, bizagi
A.9.3.1	Implementar una herramienta de gestión de la información de autenticación secreta para reducir la cantidad de este tipo de información que los usuarios están obligados a proteger.			Personal que realiza labores de TIC, oficina de control interno	Gerencia CGT	Computadora
A.11.1.1	Fortalecer la seguridad donde se ubica la sala de servidores con la edificación de una pared.			Gerencia de administración y finanzas (gaf)	Gerencia CGT	Ladrillo, cemento y mano de obra
A.11.1.2	Implementar una bitácora de acceso a la sala de servidores			Personal que realiza labores de TIC	Gerencia CGT	Bitácora
A.11.1.3	Implementar sensores de movimiento			Gerencia de administración y finanzas (gaf)	Gerencia CGT	Sensores de movimiento

Objetivos de control / controles		Fecha inicial	Fecha final	Responsable	Supervisor	Recursos
A.11.2.3	Ordenar el cableado eléctrico y de telecomunicaciones			GAF – personal que realiza labores de TIC	Gerencia CGT	Cableado electrico y de telecomunicaciones
A.11.2.4	Mejorar y documentar el proceso de mantenimiento de equipos manteniendo registros de todos los fallos, así como de todo el mantenimiento preventivo y correctivo.			Personal que realiza labores de TIC	Gerencia CGT	Computadora, bizagi
A.12.1.3	Implementar la norma técnica peruana ISO/IEC 12207:2004 en el diseño de software			GAF – personal que realiza labores de TIC	Gerencia CGT	ntp ISO/IEC 12207:2004
A.12.2.1	Instalar la última versión de software antivirus en todos los equipos del CGT.			Personal que realiza labores de TIC	Gerencia CGT	Antivirus
A.12.4.1	Establecer un registro de eventos de las actividades de los usuarios, las excepciones, fallas y eventos de seguridad de la información.			Personal que realiza labores de TIC	Gerencia CGT	Computadora
A.12.4.2	Implementar un sistema de almacenamiento para almacenar y resguardar las copias de los registros de los sistemas del CGT que necesitan ser protegidos.			Personal que realiza labores de TIC	Gerencia CGT	ISO/IEC 15489-1: 2016
A.12.4.3	Implementar un sistema de detección de intrusión, para supervisar el cumplimiento de actividades de los administradores de sistemas y de red.			GAF – personal que realiza labores de TIC	Gerencia CGT	Computadora
A.12.6.1	Establecer un proceso de gestión de vulnerabilidades técnicas para identificar riesgos asociados y las medidas asociadas a estos riesgos.			Personal que realiza labores de TIC	Gerencia CGT	Norma ISO/IEC 27031
A.12.6.2	Desarrollar e implementar una política sobre qué tipo de software puede instalar los usuarios.			Personal que realiza labores de TIC	Gerencia CGT	ISO/IEC 27002:2013, principio de privilegios mínimos.
A.13.1.1	Implementar un Firewall, IDS y IPS			GAF – personal que realiza labores de TIC	Gerencia CGT	Firewall, ids - ips
A.13.1.2	Definir niveles y acuerdos de servicios			GAF – personal que realiza labores de TIC	Gerencia CGT	Computadora
A.14.2.2	Implementar la norma técnica peruana ISO/IEC 12207:2004 en el diseño de software			Personal que realiza labores de TIC	Gerencia CGT	Ntp ISO/IEC 12207:2004
A.14.2.4	Implementar la norma técnica peruana ISO/IEC 12207:2004 en el diseño de software			Personal que realiza labores de TIC	Gerencia CGT	Ntp ISO/IEC 12207:2004

Objetivos de control / controles		Fecha inicial	Fecha final	Responsable	Supervisor	Recursos
A.18.1.3	Implementar un sistema de almacenamiento para almacenar y resguardar de manera segura los registros del CGT (Información y documentación – Registros de gestión).			Personal que realiza labores de TIC	Gerencia CGT	ISO/IEC 15489-1: 2016

4.5.6. Concientización en seguridad

Otro punto que vale la pena resaltar es que la entidad deberá seguir en su proceso de **concientización en seguridad** de la información según lo dispuesto en el Plan Operativo de Tecnologías de Información y Comunicaciones - 2018.

Se deberá capacitar a los usuarios para la correcta interpretación y su natural adaptación a los cambios implementados en el entorno, para su inserción en el sistema y su normal desarrollo de actividades, y por sobre todo para que comprenda la importancia de los cambios realizados y de su mantenimiento.

Se debe convencer al usuario de la importancia de su colaboración en el esfuerzo de mantener el entorno seguro.

Asimismo, se le debe informar de las nuevas reglas y/o políticas de la organización, la forma de trabajar para que su labor no interfiera ni perjudique el esfuerzo implicado en el proyecto de aseguramiento, los procedimientos a usar para revertir situaciones o manejar catástrofes, etc.

Se deberá dejar constancia de que el usuario fue informado respecto de las Políticas de Seguridad, y su completa comprensión, y su conformidad respecto de su cumplimiento.

La concientización hará uso de las siguientes técnicas:

a. Presentaciones grupales.
b. Manuales y folletos.
c. Cursos,
d. Coaching (un usuario experimentado capacita a un usuario inexperto).
e. Mesa de ayuda.
f. Teleconferencias.
g. Comunicados.

En todos los casos, se recomienda generar confianza de los usuarios en la persona encargada de la capacitación.

Para todas las técnicas de capacitación aquí presentadas, y las que se escapan a este trabajo, se sugiere contar con una fuerte documentación que pueda ser consultada por los usuarios, acompañada por gráficos y todo tipo de material que colabore al rápido aprendizaje e incorporación de los conceptos de seguridad.

Los usuarios deben estar conscientes de los riesgos y deben conocer su alcance e implicancias. Se les debe dar recomendaciones para el uso cotidiano de sus herramientas de trabajo y la protección de los activos de la organización.

4.5.7. Monitoreo y revisión del sistema de seguridad de la información

Este acápite se convierte en una herramienta fundamental del Sistema de Gestión de Seguridad de la Información pues consiste en la verificación de la eficacia de los controles implantados.

Un impacto nos estará probablemente diciendo que el Sistema de Gestión de Seguridad de la Información no está funcionando como estaba previsto. Con

objeto de verificar si el SGSI está funcionando según lo previsto, necesitamos: supervisar o monitorizar algo más.

a. Monitoreo y revisión de factores del riesgo.

El Comité de Seguridad de la Información deberá monitorear y revisar los riesgos y sus factores (es decir, valor de los activos, impactos, amenazas, vulnerabilidades, posibilidad de ocurrencia) para identificar cualquier cambio en el contexto de la información en una etapa temprana y para mantener una visión general de toda la imagen del riesgo; está revisión deberá realizarse cada vez que suceda y cambio importante en el contexto hay que tener claro que los riesgos no son estáticos; las amenazas, vulnerabilidades, posibilidades o consecuencias pueden cambiar abruptamente sin ninguna indicación. Por lo tanto, es necesario el monitoreo constante para detectar estos cambios. Esto lo pueden apoyar servicios externos que provean información respecto a nuevas amenazas o vulnerabilidades.

El Comité de Seguridad de la Información instaurado en el CGT deberá asegurar que se monitoree (anualmente o cuando la situación lo amerite) lo siguiente:

- Nuevos activos que hayan sido incluidos en el alcance de la gestión del riesgo.
- La modificación necesaria de los valores de los activos, por ejemplo: debido a las necesidades cambiantes del negocio.
- Nuevas amenazas que podrían ser activas tanto fuera como dentro de la organización y que no se han evaluado.
- La posibilidad de que las vulnerabilidades nuevas o aumentadas permitan que haya amenazas que exploten estas vulnerabilidades nuevas o cambiadas.
- Vulnerabilidades identificadas para determinar las que se están exponiendo a amenazas nuevas o re-emergentes.
- El mayor impacto o las consecuencias de amenazas, vulnerabilidades y riesgos evaluados resultan en un nivel de riesgo inaceptable cuando se agregan.
- Incidentes de seguridad de la información.

Las nuevas amenazas, vulnerabilidades o cambios en las posibilidades o las consecuencias pueden incrementar los riesgos previamente evaluados como bajos. La revisión de riesgos bajos y aceptados debe considerar cada riesgo por separado y todos los riesgos como un agregado también para evaluar su impacto acumulado potencial. Si los riesgos no caen dentro de la categoría baja o aceptable, se les debe tratar utilizando una o más de las opciones en el tratamiento de riesgo en la seguridad de la información.

Los factores que afectan las posibilidades y las consecuencias de que ocurran las amenazas pueden cambiar, así como pueden cambiar los factores que afectan la conveniencia o el costo de las distintas opciones de tratamiento.

El resultado de las actividades de monitoreo del riesgo pueden ser un

insumo para otras actividades de revisión del riesgo.

Queda claro que CGT deberá revisar todo el Sistema de Gestión de Seguridad de la Información a intervalos anuales o cuando ocurran cambios importantes que repercutan en el mismo.

También se medirá la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:

- La organización.
- Tecnología.
- Objetivos y procesos comerciales.
- Amenazas identificadas.
- Efectividad de los controles implementados.
- Eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

b. Auditorías internas SGSI

El CGT a cargo de la oficina de Control Interno deberá realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

- Cumplen con los requerimientos de este Estándar Internacional y la legislación y regulaciones relevantes.
- Cumplen con los requerimientos de seguridad de la información identificados.
- Se implementan y mantienen de manera efectiva.
- Se realizan conforme lo esperado.

Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de auditoría. La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros se deben definir en un procedimiento documentado.

La Gerencia CGT y Jefaturas responsables para el área siendo auditada deben asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación.

4.5.8. Validación de la propuesta

De acuerdo al tipo de investigación, que en este caso es descriptiva propositiva, se plantea hipótesis. Sin embargo, el modelo propuesto fue validado mediante una encuesta de opinión por parte de los usuarios de TI del CGT, que permita medir los siguientes indicadores:

Tabla N° 57 Indicadores para la validación del modelo propuesto

Indicador
Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos internos del CGT.
Nivel de satisfacción de las necesidades y expectativas de las partes interesadas
Nivel de conformidad del alcance del SGSI
Nivel de cumplimiento de los requisitos de la Norma NTP 27001:2014
Nivel de compromiso de la alta gerencia
Nivel Efectividad de las políticas de TI
Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.
Nivel de Efectividad de las acciones para tratar los riesgos
Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.

a. Población y muestra de estudio

Unidad de Análisis: Usuarios de los servicios de TI ofrecidos por la Oficina de Tecnología de la Información del CGT.

Población: La población de la investigación está conformada de la siguiente manera:

Tabla N° 58 Distribución de usuarios de TI en el CGT

Tipo de usuario	N° Usuarios
Personal Directivo (autoridades y responsables de jefaturas)	12
Personal Administrativo (secretarias, administrativo)	21
Total	33

Fuente: Plan Operativo Institucional del CGT

Muestra: Como la población es pequeña, la muestra será la población.

b. Herramienta de recopilación de información

Se aplicó una encuesta de satisfacción sobre el Sistema de Gestión de la Seguridad de la Información propuesto a la muestra de la población indicada. Esta encuesta fue diseñada de tal forma que sea compatible con los indicadores que se desean evaluar en esta investigación. Para ello se elaboró la siguiente tabla que muestra la relación de las preguntas diseñadas en la encuesta con los correspondientes indicadores que permiten medirlo con la información recopilada.

Tabla N° 59 Matriz de consistencia entre los indicadores y las preguntas de la encuesta

Dim.	Indicador	Pregunta	
Contexto de la organización	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos internos del CGT.	P1	Usted considera que el Sistema de Gestión de Seguridad de la Información se adecuada a la estructura organizativa, a la normativa interna y a los procesos internos del CGT.
	Nivel de satisfacción de las necesidades y expectativas de las partes interesadas	P2	El SGSI propuesto permite satisfacer las necesidades y expectativas de las partes interesadas en la gestión de la seguridad de la información.
	Nivel de conformidad del alcance del SGSI	P3	Usted está conforme del modo como se determinó el alcance del Sistema de Gestión de Seguridad de la Información propuesto.
	Nivel de cumplimiento de los requisitos de la Norma NTP 27001:2014	P4	En qué grado usted cree que el SGSI propuesto cumple con las exigencias o los requisitos de la Norma Técnica Peruana 27001: 2014.
Liderazgo	Nivel de compromiso de la alta gerencia	P5	Cree usted que en el SGSI propuesto se han establecido con claridad los liderazgos y compromisos para un adecuado gobierno de la seguridad de la información en el CGT.
	Nivel Efectividad de las políticas de TI	P6	Usted cree que la declaración de las políticas de seguridad en el SGSI permite establecer los objetivos de seguridad y permite la mejora continua del mismo.
	Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.	P7	Usted cree que los roles, responsabilidades y autoridades organizacionales del SGSI son adecuadas para la gestión de la seguridad de la información en el CGT.
Planificación	Nivel de Efectividad de las acciones para tratar los riesgos	P8	Considera usted que se definió y aplico adecuadamente un proceso de valorización del riesgo de seguridad de la información
	Nivel de Efectividad de las acciones para tratar los riesgos	P9	Considera usted que se definió y aplico adecuadamente un proceso de tratamiento de riesgo de seguridad de la información
	Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.	P10	Usted cree que los objetivos de seguridad de la información y su plan de ejecución planteados en el SGSI son adecuados para la gestión de la seguridad de la información en el CGT.
Grado de satisfacción de la identificación y tratamiento de los riesgos identificados		P11	Según usted cuál es su nivel de satisfacción de que el SGSI propuesto logra gestionar los riesgos reales y potenciales de TI.

c. Fiabilidad del instrumento (encuesta)

Se determinó el nivel de fiabilidad del instrumento (la encuesta) utilizando el estadístico Alfa de Cronbach. El método de consistencia interna basado en el alfa de Cronbach permite estimar la fiabilidad de un instrumento de medida a través de un conjunto de ítems que se espera que midan el mismo constructo o dimensión teórica. La validez de un instrumento se refiere al

grado en que el instrumento mide aquello que pretende medir. Y la fiabilidad de la consistencia interna del instrumento se puede estimar con el alfa de Cronbach. La medida de la fiabilidad mediante el alfa de Cronbach asume que los ítems (medidos en escala tipo Likert) miden un mismo constructo y que están altamente correlacionados (Welch & Comer, 1988). Cuanto más cerca se encuentre el valor del alfa a 1 mayor es la consistencia interna de los ítems analizados. La fiabilidad de la escala debe obtenerse siempre con los datos de cada muestra para garantizar la medida fiable del constructo en la muestra concreta de investigación.

Procesados los datos se obtuvo lo siguiente:

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,877	11

		N	%
Casos	Válidos	22	100,0
	Excluidos[a]	0	,0
	Total	22	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Como criterio general, George & Mallery (2003) sugieren las recomendaciones siguientes para evaluar los coeficientes de Alfa de Cronbach:

- Coeficiente alfa >0.9 es excelente
- Coeficiente alfa >0.8 es bueno
- Coeficiente alfa >0.7 es aceptable
- Coeficiente alfa >0.6 es cuestionable
- Coeficiente alfa >0.5 es pobre
- Coeficiente alfa <0.5 es inaceptable

Es este caso se ha alcanzado 0.877, confirmándose que la encuesta aplicada es buena.

d. Análisis de la Regresión Múltiple

Utilizamos regresión múltiple porque nuestra hipótesis pretende estudiar la posible relación entre las variables independientes (predictoras o explicativas) y la variable dependiente (criterio, explicada, respuesta). En este caso, nuestras variables son:

- Variable Independiente (X_i): Sistema de Gestión de la Seguridad de la Información, basado en la NTP ISO/IEC 27001:2014, descrita a través

de las dimensiones de contexto de la organización (X_1), liderazgo (X_2) y Planificación (X_3)

- Variable dependiente (Y): Grado de satisfacción de la identificación y tratamiento de los riesgos identificados

Por tanto, el modelo a evaluar es un modelo de regresión múltiple de la forma:

$$Y = C0 + C1X1 + C2X2 + C3X3 + e$$

Esto significa que se pretende evaluar la relación existente entre la variable dependiente "Riesgos reales y potenciales de la Seguridad de la Información" y la variable independiente "Sistema de Gestión de la Seguridad de la Información, basado en la NTP ISO/IEC 27001:2014", esta última explicada por tres dimensiones: Contexto de la organización (X1), liderazgo (X2) y Planificación (X3)

Para lograr este objetivo, se desarrolló el siguiente procedimiento:

- **Reducción de ítems de cada dimensión evaluada**

  Dado que cada una de las dimensiones tiene más de un ítem a evaluar (ver Tabla N° 60) se tuvo que reducir a un solo ítem, de la siguiente manera:

Tabla N° 60 Matriz de reducción de ítems evaluados

Dimensión	Ítem		Ítem reducido
Contexto de la organización(X_1)	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos internos del CGT.	P1	Dim_contexto = (P1 + P2 + P3 + P4)/4
	Nivel de satisfacción de las necesidades y expectativas de las partes interesadas	P2	
	Nivel de conformidad del alcance del SGSI	P3	
	Nivel de cumplimiento de los requisitos de la Norma NTP 27001:2014	P4	
Liderazgo(X_2)	Nivel de compromiso de la alta gerencia	P5	Dim_liderazgo = (P5 + P6 + P7)/3
	Nivel Efectividad de las políticas de TI	P6	
	Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.	P7	
Planificación(X_3)	Nivel de Efectividad de las acciones para tratar los riesgos	P8	Dim_planificacion = (P8 + P9 + P10)/3
	Nivel de Efectividad de las acciones para tratar los riesgos	P9	
	Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos	P10	

- **Análisis de regresión múltiple**

Para nuestro análisis se aplicará la metodología de regresión múltiple jerárquica con tres bloques, donde se fueron tomando variable por variable independiente con las que estamos trabajando, con la finalidad de generar diferentes modelos. Los modelos que esperamos generar son los siguientes:

Modelo 1: sólo con la variable Contexto de la organización(X1)

Modelo 2: sólo con las variables Contexto de la organización (X1) y Liderazgo (X2)

Modelo 3: con las tres variables Contexto de la organización (X1), Liderazgo (X2) y Planificación (X3)

Esto nos permitirá identificar mayor información de las variables independientes con las que estamos trabajando; así como también nos permite identificar si alguna de esas variables independientes no aporta al modelo, por tanto puede ser excluida del modelo.

Los resultados obtenidos se muestran a continuación:

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Durbin-Watson
1	,569[a]	,344	,335	,468	
2	,611[b]	,387	,356	,460	
3	,713[c]	,523	,478	,415	1,571

a. Variables predictoras: (Constante), Dim_contexto

b. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo

c. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo, Dim_planificacion

Del cuadro se deduce que:

- El Modelo 1 (sólo con la variable Contexto de la organización (X_1)) explica el 34.4% de la varianza de la variable dependiente.
- El Modelo 2 (sólo con las variables Contexto de la organización (X_1) y Liderazgo (X_2)) explica el 38.7% de la varianza de la variable dependiente.
- El Modelo 3 (con las tres variables Contexto de la organización (X_1), Liderazgo (X_2) y Planificación (X_3)) explica el 52.3% de la varianza de la variable dependiente.

Para efectos de la demostración de la hipótesis seleccionamos el Modelo 3 donde se incluyen las tres variables independientes.

Por otro lado, en el mismo cuadro observamos el resultado de la prueba de Durbin-Watson que nos da un valor para determinar la independencia de errores, pero no una significancia; por lo que tenemos

que tener algunos criterios de identificación de cuando este valor es bueno o no bueno. El valor esperado de la prueba Durbin-Watson es que sea lo más cercano a 2, en este caso tenemos un valor de 1.571 que es bueno. El rango que se debe tener en cuenta para aceptar el resultado de la prueba de Durbin-Watson es 1 ± 2, es decir entre 1 y 3.

La interpretación de este resultado es que no existe dependencia de las observaciones recogidas, por lo tanto se demuestra que la recogida de la información ha sido aleatoria, evitando así invalidar por completo las conclusiones del análisis estadístico.

- **Análisis de varianza (ANOVA)**

Los resultados del ANOVA se muestran en el siguiente cuadro:

Modelo		Suma de cuadrados	Gl	Media cuadrática	F	Sig.
1	Regresión	3,331	1	3,524	15,003	,000[b]
	Residual	6,455	27	,219		
	Total	9,781	26			
2	Regresión	3,934	2	1,971	9,289	,001[c]
	Residual	5,831	26	,212		
	Total	9,862	29			
3	Regresión	5,210	3	1,744	9,802	,000[d]
	Residual	4,623	26	,172		
	Total	9,779	29			

a. Variable dependiente: P11

b. Variables predictoras: (Constante), Dim_contexto

c. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo

d. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo, Dim_planificacion

Como el modelo de regresión que estamos trabajando es saber si las tres variables independientes están prediciendo la variable dependiente, entonces nos quedamos con los resultados del último modelo (Modelo 3) que se muestra en la tabla ANOVA.

Aquí se observa que hay una significancia menor al 0.05 (0.00 ≤ 0.05) y la interpretación en términos de hipótesis es que el modelo que estamos probando mejora significativamente la predicción de la variable dependiente.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

A partir del desarrollo del proyecto se concluye lo siguiente:

1. El modelo propuesto se valida con un 52% de aceptación. Lo que significa que para los usuarios de TI de CGT el modelo de sistema de Gestión de Seguridad de la Información, basado en la NTP ISO/IEC 27001:2014 planteado, permite minimizar los riesgos reales y potenciales de la seguridad de la información en el CGT.
2. Así mismo el modelo propuesto con las 3 dimensiones evaluadas, en la que se explica la varianza de la variable dependiente en 52%, señala que falta casi un 50% de explicación de la varianza de la variable dependiente, por lo que sería conveniente realizar otras investigaciones para encontrar otras dimensiones que explique mejor el modelo propuesto.
3. Según el diagnóstico de la situación actual de la seguridad de la información realizada, nos muestra que el nivel de cumplimiento del CGT frente a los requerimientos de la NTP ISO/IEC 27002:2005, es del 30%, lo que significa que la implementación del Sistema de Gestión de Seguridad de la información le implicará a la institución un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos.
4. Así mismo el modelo de Sistema de Gestión de Seguridad de la Información planteado tomo en cuenta los requerimientos mínimos que la ONGEI exige, los cuales son: En la Fase de Organización (Obtener apoyo institucional, determinar el alcance de SGSI, determinar la declaración de Política de Seguridad de la Información y objetivos, determinar criterios para la evaluación y aceptación de riesgos) y en la Fase de Planificación (Realizar evaluación de riesgos, desarrollar un plan de tratamiento de riesgos y desarrollar la declaración de aplicabilidad).
5. Se tomó en cuenta los postulados de la NTP ISO/IEC 27001:2014 los cuales nos dan como resultado los diferentes formatos que fueron presentados a la Gerencia y los cuales pueden ser visualizados en los anexos de este estudio.
6. Para que este proyecto tenga éxito, es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con el apoyo de la Gerencia de modo que se facilite el acceso a la información de todas las áreas pertinentes.
7. Para contrarrestar la falta de concientización de seguridad de la información se deberá incluir sesiones de capacitación en las que se concientice al personal sobre la importancia de la información con la cual se realizan las labores institucionales, así como fomentar el cumplimiento de las políticas que garantice la seguridad de la misma.
8. Es probable que la implantación de las nuevas condiciones de empleo para los colaboradores antiguos sea recibida con rechazo dado que muchos de ellos se encuentran trabajando mucho tiempo en la institución y puedan percibir este cambio como una amenaza. Este posible obstáculo deberá ser debidamente manejado en conjunto con el área de recursos humanos.

5.2. Recomendaciones y trabajos futuros

1. Para lograr una efectiva implementación del Sistema de Gestión de Seguridad de Información en el CGT, se recomienda seguir con los siguientes factores de éxito; en primer lugar seguir teniendo el apoyo constante de la Gerencia, segundo, seguir con el diseño del SGSI planteado, el cual se desarrolló a lo largo del proyecto; y tercero, generar conciencia en la institución. Este último aspecto no siempre se logra de inmediato, pues muchas personas se muestran reacias al cambio, lo que puede ocasionar inconvenientes en la implementación del SGSI.
2. Por ello, es necesario generar una cultura de seguridad dentro de la institución, es decir concientizar a cada colaborador de la importancia de sus actividades de seguridad de información y la manera de cómo contribuye a los objetivos del SGSI, se recomienda realizar capacitaciones permanentes a todo el personal del CGT.
3. Se recomienda establecer, como mínimo, reuniones mensuales del comité de seguridad de la información, el cual fue propuesto en este estudio para dar un seguimiento adecuado a cada uno de los avances realizados en el sistema de gestión, así como ir aumentando de manera progresiva el alcance del mismo para lograr asegurar, a corto plazo, la información de todo el CGT.
4. Es importante que se defina el cargo del Oficial de Seguridad de la Información, en conjunto con el área de Seguridad de la Información los cuales deberían pertenecer a alguna de las direcciones institucionales o conformar una nueva, de modo que tenga un nivel de acción más alto que el de las demás direcciones y reporte directamente a la Gerencia. Esta localización en la estructura organizacional es necesaria puesto que el SGSI requiere que se garantice el cumplimiento de las políticas definidas, así como el apoyo de todas las áreas de la institución.
5. El CGT requiere implementar una serie de controles con el objetivo de fortalecer su seguridad y poder dar cumplimiento a los requerimientos establecidos en la norma NTP ISO/IEC 27001:2014, por eso es fundamental que lleven a cabo los diferentes planes de acciones que se definieron en el presente trabajo de grado.
6. Es necesario que la Gerencia de Tecnología de la Información revise su capacidad con el objetivo de garantizar la debida implementación de los controles y planes de acciones que se requieren llevar a cabo para cerrar las brechas encontradas producto de los diagnósticos realizados, ya que algunos de estos planes de acción requiere de componente tecnológico.
7. Es pertinente que la institución evalué la vialidad de algunos planes de acciones propuestos, debido a que su implementación demanda la adquisición de herramientas y/o soluciones tecnológicas que implica adelantar procesos de contratación para su adquisición. Algunas de las soluciones tecnológicas que se proponen, pueden llegar a tener un costo elevado y/o su implementación puede demandar un tiempo considerable.
8. Así mismo es necesario que el CGT asigne un presupuesto orientado a la implementación de los controles del SGSI, así como para las capacitaciones y charlas de concientización, los servicios de consultoría y las revisiones anuales que se darán para asegurar la continuidad del sistema.

9. Se recomienda que para diseñar, implementar e implantar adecuadamente el SGSI, se utilicen estándares y buenas prácticas que sean ampliamente aceptadas. No necesariamente se tiene que aplicar lo que se ha mostrado en este documento, ya que existen varias herramientas de buenas prácticas, como ITIL para implementar un SGSI. Es importante usar los estándares y buenas prácticas de guía, pero no se debe implementar todo de la manera indicada. La implementación va a depender de las necesidades del CGT. Cabe resaltar que estos estándares indican que es aquello que se debe controlar, pero no indica el cómo.
10. También, se propone como trabajo futuro el diseño e implementación de un sistema de gestión de continuidad de negocio, debido a que no existe en la organización y es motivo de observación continua por parte de auditoria externa.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre Freire, D. S., & Palacios Cruz, J. C. (2014). *Evaluación técnica de seguridades del data center del municipio de Quito según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005.* Ecuador: Universidad de las fuerzas armadas ESPE, Sede SANGOLQUI.

Aguirre Mollehuanca, D. A. (2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S:A. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Alcántara Torres, J. C. (2015). Guía de implementación de La seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte PNP en la ciudad de Chiclayo. Universidad Catolica Santo Toribio de Mogrovejo.

BSI Group México . (s/a). Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013. *ISO/IEC 27001 – Gestión de Seguridad de la Información – Guía de Transición*.

Carrasco, C. A. (2010). *Impacto del riesgo en el gobierno de las tecnologias de Información y comunicación en la gestión empresarial industrial del sigo XXI.* Lima-Perú.

Caviedes Sanabria, F., & Prado Urrego, B. A. (2012). *Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización.* Santiago de Cali.

Concha Huacoto, N. E. (2005). Propuesta para implantar CMMI en una empresa con multiples unidades desarrolladoras de software. *Tesis pregrado*. Lima: Universidad Nacioanl Mayor de San Marcos.

Condori Alejo, H. I. (2012). Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario. *tesis postgrado*. Lima: Universidad Inca Garcilaso de la Vega.

De la Cruz Guerrero, C. W., & Vasquez Montenegro, J. C. (2008). Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información(SGSI) para la realidad Tecnólogica de la USAT. *tesis pregrado*. Chiclayo: Universidad Catolica Santo Toribio de Mogrovejo.

Enriquez Espinosa, P. R. (2013). *Implementación de los controles asignados al dominio "Gestión De Activos", bajo los lineamientos establecidos por la norma ISO/IEC 27001 anexo a, para las empresas Municipales de Cali, Emcali E.I.C.E-ESP.* Colombia: Universidad Autónoma de Occidente.

Espinoza Aguinaga, H. R. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Hernández Pinto, M. G. (2006). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. *tesis pregrado*. Guayaquil - Ecuador: Escuela Superior Politécnica del Litoral.

Huamán Monzón, F. M. (2014). Diseño De Procedimientos De Auditoría De Cumplimiento De La Norma NTP-ISO/IEC 27002:2005 Como Parte Del Proceso De Implantación De La Norma Técnica NTP-ISO/IEC 27001:2008 En Instituciones Del Estado Peruano. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Inteco. (s/a). Implantación de un SGSI en la empresa. *SGSI*, 22.

ISO 27000.es. (2005). *ISO 27000*. Recuperado el 15 de 03 de 2016, de ISO 27000: www.iso27000.es

ISO/IEC 27001. (2005). *Tecnología de la Informacion-Tecnicas de Seguridad-Sistemas de gestión de seguridad de la Información - Requerimientos.* Primera edicion 2005-10-15.

ISO/IEC 27002. (2013). *Information technology - Security techniques - Code of practice for information security management.* EEUU.

ISOTools Excellence. (17 de 01 de 2014). *http://www.pmg-ssi.com*. Obtenido de http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

ISOTools Excellence. (31 de 01 de 2014). *http://www.pmg-ssi.com/*. Obtenido de http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

Ladino A., M. I., Villa S., P. A., & López E., A. M. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia et Technica Año XVII*, 334.

López M., A. A. (2011). *Diseño de un Plan de Gestión de Seguridad de la Información. Caso: Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara.* Venezuela: Universidad Centoccidental “Lisandro Alvarado”.

Magerit. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciónes Públicas.

Mancera, S. (. (2011). Perspectivas sobre los riesgos de TI. *Seguridad de la información en un mundo sin fronteras*, 15.

Mega, I. G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Montevideo, Uruguay.

Montesino Perurena, R., Baluja Garcia, W., & Porven Rubier, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista de Ingenieria Electrónica Automática y Comunicaciones*.

NTP ISO/IEC 27002. (2007). *EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.* Lima.

NTP ISO/IEC 27001. (2016). *EDI Tecnologia de la Información. Tecnicas de seguridad. Sistemas de gestión de seguridad de la información.* Lima.

NTP-ISO/IEC 27001. (2014). *EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.* Lima.

NTP-ISO/IEC 27005. (2009). *EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información.* Lima, Perú.

Ozier, W. (2004). *Risk Analysis and Assessment" Information Security Management Handbook. 5th edition.* USA: Auerbach Publications.

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals.* USA: Auerbach Publications.

Portal Oficial de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI. (NTP ISO/IEC 27001:2008). Obtenido de http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

Poveda, J. M. (s/a). *Auditoría Informática.* UNI-NORTE.

Reina García, E., & Morales Ramírez , J. R. (2014). Modelamiento de procesos basados en el grupo de normas internacionales ISO/IEC 27000 para gestionar el riesgo y seleccionar controles en la implementación del sistema de gestión de seguridad de la información. *tesis pregrado*. Universidad tecnológica de Pereira Facultad de ingenierías eléctrica, electrónica, física y ciencias de la computación.

Robles , R., & Rodriguez de Roa, Á. (2006). La gestión de la seguridad en la empresa. *Comite de Entidades de Certificación de la AEC*, 14-18.

Talavera Álvarez, V. R. (2015). *Diseño de un Sistema de Gestión De Seguridad de la Información para una entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013.* Lima-Perú: Pontificia Universidad Católica del Perú.

Tupia Anticona, M. F. (2011). *Gobierno de las tecnologías de información bajo la óptica de COBIT.* Perú: Tupia Consultores y Auditores S.A.C. Perú.

Universidad Distrital Franscisco José de Caldas. (s/a). Gestión del riesgo. En *Proceso de desarrollo Open UP/OAS* (pág. Cap. 5).

Villalón Huerta, A. (2002). *SEGURIDAD EN UNIX Y REDES Version 2.1.*

Welch, S., & Comer, J. (1988). *Quantitative methods for public administration: techniques and applications* (2, reimpresa ed.). (1. Brooks/Cole Pub. Co., Ed.) la Universidad de Virginia.

ANEXOS

ANEXO N° 01 – Cuestionario NTP ISO/IEC 27002: 2007

Nivel	CMM	Porcentaje	Descripción
Inexistente	L0	0%	- Carencia completa de cualquier proceso reconocible. - No se ha reconocido siquiera que existe un problema a resolver.
Inicial / Ad-hoc	L1	10%	- Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. - Los procedimientos son inexistentes o localizados en áreas concretas - No existen plantillas definidas a nivel corporativo.
Reproducible, pero intuitivo	L2	50%	- Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. - Se normalizan las buenas prácticas en base a la experiencia y al método. - No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. - Se depende del grado de conocimiento de cada individuo.
Proceso definido	L3	90%	- La organización entera participa en el proceso. - Los procesos están implantados, documentados y comunicados mediante entrenamiento.
Gestionado y medible	L4	95%	- Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. - Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
Optimizado	L5	100%	- Los procesos están bajo constante mejora. - En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.
No Aplica	-	N/A	- El control no es aplicable al CGT.

ANEXO N° 02 – Resultado del Cuestionario NTP ISO/IEC 27002: 2007

CONTROLES NTP ISO/IEC 27002:2005			Efectividad	% Efectividad
Clausula	**SEC**	**Control/Objetivo de Control**		
5. Política de Seguridad	5.1	Política de seguridad de la información		10%
	5.1.1	Documento de política de seguridad de la información	Inicial / Ad-hoc	10%
	5.1.2	Revisión de la política de seguridad de la información	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**10%**
6. Aspectos Organizativos de la seguridad de la información	6.1	Organización Interna		35%
	6.1.1	Compromiso de la Dirección con la seguridad de la información.	Reproducible, pero intuitivo	50%
	6.1.2	Coordinación de la seguridad de la información.	Inicial / Ad-hoc	10%
	6.1.3	Asignación de responsabilidades relativas a la seguridad de la información.	Reproducible, pero intuitivo	50%
	6.1.4	Proceso de autorización de recursos para el tratamiento de la información.	Inicial / Ad-hoc	10%
	6.1.5	Acuerdos de confidencialidad.	Reproducible, pero intuitivo	50%
	6.1.6	Contacto con las autoridades.	Reproducible, pero intuitivo	50%
	6.1.7	Contacto con grupos de especial interés.	Inicial / Ad-hoc	10%
	6.1.8	Revisión independiente de la seguridad de la información	Reproducible, pero intuitivo	50%
	6.2	Seguridad en los accesos de terceras partes		23%
	6.2.1	Identificación de los riesgos derivados del acceso de terceros.	Reproducible, pero intuitivo	50%
	6.2.2	Tratamiento de la seguridad en la relación con los clientes.	Inicial / Ad-hoc	10%
	6.2.3	Tratamiento de la seguridad en contratos con terceros.	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**31%**
7. Clasificación y Control de Activos	7.1	Responsabilidad sobre los activos.		50%
	7.1.1	Inventario de activos.	Proceso definido	90%
	7.1.2	Propiedad de los activos.	Reproducible, pero intuitivo	50%
	7.1.3	Uso aceptable de los activos.	Inicial / Ad-hoc	10%
	7.2	Clasificación de la información.		30%
	7.2.1	Directrices de clasificación.	Reproducible, pero intuitivo	50%
	7.2.2	Etiquetado y manipulado de la información.	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**41%**
8. Seguridad en Recursos Humanos	8.1	Seguridad antes del empleo.		90%
	8.1.1	Funciones y responsabilidades.	Proceso definido	90%
	8.1.2	Investigación de antecedentes.	Proceso definido	90%
	8.1.3	Términos y condiciones de contratación.	Proceso definido	90%
	8.2	Durante el empleo.		37%
	8.2.1	Responsabilidades de la Dirección.	Inicial / Ad-hoc	10%
	8.2.2	Concienciación, formación y capacitación en seguridad de la información.	Inicial / Ad-hoc	10%
	8.2.3	Proceso disciplinario.	Proceso definido	90%
	8.3	Finalización o cambio del empleo.		50%
	8.3.1	Responsabilidad del cese o cambio.	Proceso definido	90%
	8.3.2	Devolución de activos.	Inicial / Ad-hoc	10%

	8.3.3	Retirada de los derechos de acceso.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**59%**
9. Seguridad Física y del Entorno	9.1	Áreas seguras.		30%
	9.1.1	Perímetro de seguridad física.	Reproducible, pero intuitivo	50%
	9.1.2	Controles físicos de entrada.	Inicial / Ad-hoc	10%
	9.1.3	Seguridad de oficinas, despachos e instalaciones.	Inicial / Ad-hoc	10%
	9.1.4	Protección contra las amenazas externas y de origen ambiental.	Inicial / Ad-hoc	10%
	9.1.5	Trabajo en áreas seguras.	Reproducible, pero intuitivo	50%
	9.1.6	Áreas de acceso público y de carga y descarga.	Reproducible, pero intuitivo	50%
	9.2	Seguridad de los equipos.		16%
	9.2.1	Emplazamiento y protección de equipos.	Inicial / Ad-hoc	10%
	9.2.2	Instalaciones de suministro.	Inicial / Ad-hoc	10%
	9.2.3	Seguridad del cableado.	Inicial / Ad-hoc	10%
	9.2.4	Mantenimiento de los equipos.	Reproducible, pero intuitivo	50%
	9.2.5	Seguridad de los equipos fuera de las instalaciones.	Inicial / Ad-hoc	10%
	9.2.6	Reutilización o retirada segura de equipos.	Inicial / Ad-hoc	10%
	9.2.7	Retirada de materiales propiedad de la empresa.	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**22%**
10. Gestión de Comunicaciones y operaciones	10.1	Responsabilidades y procedimientos de operación.		10%
	10.1.1	Documentación de los procedimientos de operación.	Inicial / Ad-hoc	10%
	10.1.2	Gestión de cambios.	Inicial / Ad-hoc	10%
	10.1.3	Segregación de tareas.	Inicial / Ad-hoc	10%
	10.1.4	Separación de los recursos de desarrollo, prueba y operación.	Inicial / Ad-hoc	10%
10. Gestión de Comunicaciones y operaciones	10.2	Gestión de la provisión de servicios.		10%
	10.2.1	Provisión de servicios.	Inicial / Ad-hoc	10%
	10.2.2	Supervisión y revisión de los servicios prestados por terceros.	Inicial / Ad-hoc	10%
	10.2.3	Gestión del cambio en los servicios prestados por terceros.	Inicial / Ad-hoc	10%
	10.3	Planificación y aceptación del sistema.		10%
	10.3.1	Gestión de capacidades.	Inicial / Ad-hoc	10%
	10.3.2	Aceptación del sistema.	Inicial / Ad-hoc	10%
	10.4	Protección contra el código malicioso y descargable.		50%
	10.4.1	Controles contra el código malicioso.	Reproducible, pero intuitivo	50%
	10.4.2	Controles contra el código descargado en el cliente.	Reproducible, pero intuitivo	50%
	10.5	Copias de seguridad.		50%
	10.5.1	Copias de seguridad de la información.	Reproducible, pero intuitivo	50%
	10.6	Gestión de seguridad en redes.		50%
	10.6.1	Controles de red.	Reproducible, pero intuitivo	50%
	10.6.2	Seguridad de los servicios de red.	Reproducible, pero intuitivo	50%
	10.7	Manipulación de los soportes.		28%
	10.7.1	Gestión de soportes extraíbles.	Inexistente	0%
	10.7.2	Retirada de soportes.	Reproducible, pero intuitivo	50%
	10.7.3	Procedimientos de manipulación de la información.	Inicial / Ad-hoc	10%

	10.7.4	Seguridad de la documentación del sistema.	Reproducible, pero intuitivo	50%
	10.8	Intercambio de información.		26%
	10.8.1	Políticas y procedimientos de intercambio de información.	Inicial / Ad-hoc	10%
	10.8.2	Acuerdos de intercambio.	Inicial / Ad-hoc	10%
	10.8.3	Soportes físicos en tránsito.	Inicial / Ad-hoc	10%
	10.8.4	Mensajería electrónica.	Reproducible, pero intuitivo	50%
	10.8.5	Sistemas de información empresariales.	Reproducible, pero intuitivo	50%
	10.9	Servicios de comercio electrónico.		50%
	10.9.1	Comercio electrónico.	No Aplica	N/A
	10.9.2	Transacciones en línea.	No Aplica	N/A
	10.9.3	Información públicamente disponible.	Reproducible, pero intuitivo	50%
	10.10	Supervisión.		10%
	10.10.1	Registros de auditoría.	Inicial / Ad-hoc	10%
	10.10.2	Supervisión del uso del sistema.	Inicial / Ad-hoc	10%
	10.10.3	Protección de la información de los registros.	Inicial / Ad-hoc	10%
	10.10.4	Registros de administración y operación.	Inicial / Ad-hoc	10%
	10.10.5	Registro de fallos.	Inicial / Ad-hoc	10%
	10.10.6	Sincronización del reloj.	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**25%**
11. Control de Acceso	11.1	Requisitos de negocio para el control de acceso.		50%
	11.1.1	Política de control de acceso.	Reproducible, pero intuitivo	50%
	11.2	Gestión de acceso de usuario.		50%
	11.2.1	Registro de usuario.	Reproducible, pero intuitivo	50%
	11.2.2	Gestión de privilegios.	Reproducible, pero intuitivo	50%
	11.2.3	Gestión de contraseñas de usuario.	Reproducible, pero intuitivo	50%
	11.2.4	Revisión de los derechos de acceso de usuario.	Reproducible, pero intuitivo	50%
	11.3	Responsabilidades de los usuarios.		37%
	11.3.1	Uso de contraseñas.	Reproducible, pero intuitivo	50%
	11.3.2	Equipo de usuario desatendido.	Reproducible, pero intuitivo	50%
	11.3.3	Política de puesto de trabajo despejado y pantalla limpia.	Inicial / Ad-hoc	10%
	11.4	Control de acceso a la red.		39%
	11.4.1	Política de uso de los servicios en red.	Reproducible, pero intuitivo	50%
	11.4.2	Autenticación de usuario para conexiones externas.	Reproducible, pero intuitivo	50%
	11.4.3	Identificación de los equipos en las redes.	Reproducible, pero intuitivo	50%
	11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	Reproducible, pero intuitivo	50%
	11.4.5	Segregación de las redes.	Inicial / Ad-hoc	10%
	11.4.6	Control de la conexión a la red.	Inicial / Ad-hoc	10%
	11.4.7	Control de encaminamiento (routing) de red.	Reproducible, pero intuitivo	50%
	11.5	Control de acceso al sistema operativo.		40%
	11.5.1	Procedimientos seguros de inicio de sesión.	Reproducible, pero intuitivo	50%
	11.5.2	Identificación y autenticación de usuario.	Reproducible, pero intuitivo	50%
	11.5.3	Sistema de gestión de contraseñas.	Proceso definido	90%

	11.5.4	Uso de los recursos del sistema.	Reproducible, pero intuitivo	50%
	11.5.5	Desconexión automática de sesión.	Inexistente	0%
	11.5.6	Limitación del tiempo de conexión.	Inexistente	0%
	11.6	Control de acceso a las aplicaciones y a la información.		50%
	11.6.1	Restricción del acceso a la información.	Reproducible, pero intuitivo	50%
	11.6.2	Aislamiento de sistemas sensibles.	Reproducible, pero intuitivo	50%
	11.7	Ordenadores portátiles y teletrabajo.		
	11.7.1	Ordenadores portátiles y comunicaciones móviles.	No Aplica	N/A
	11.7.2	Teletrabajo.	No Aplica	N/A
			Efectividad conjunta:	**43%**
12. Adquisición, desarrollo y mantenimiento de Sistemas de Información	12.1	Requisitos de seguridad de los sistemas de información.		50%
	12.1.1	Análisis y especificación de los requisitos de seguridad.	Reproducible, pero intuitivo	50%
	12.2	Tratamiento correcto de las aplicaciones.		40%
	12.2.1	Validación de los datos de entrada.	Reproducible, pero intuitivo	50%
	12.2.2	Control del procesamiento interno.	Reproducible, pero intuitivo	50%
	12.2.3	Integridad de los mensajes.	Inicial / Ad-hoc	10%
	12.2.4	Validación de los datos de salida.	Reproducible, pero intuitivo	50%
	12.3	Controles criptográficos.		
	12.3.1	Política de uso de los controles criptográficos.	No Aplica	N/A
	12.3.2	Gestión de claves.	No Aplica	N/A
	12.4	Seguridad de los archivos de sistema.		37%
	12.4.1	Control del software en explotación.	Inicial / Ad-hoc	10%
	12.4.2	Protección de los datos de prueba del sistema.	Reproducible, pero intuitivo	50%
	12.4.3	Control de acceso al código fuente de los programas.	Reproducible, pero intuitivo	50%
	12.5	Seguridad en los procesos de desarrollo y soporte.		18%
	12.5.1	Procedimientos de control de cambios.	Reproducible, pero intuitivo	50%
	12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Inexistente	0%
	12.5.3	Restricciones a los cambios en los paquetes de software.	Inicial / Ad-hoc	10%
	12.5.4	Fugas de información.	Inicial / Ad-hoc	10%
	12.5.5	Externalización del desarrollo de software.	No Aplica	N/A
	12.6	Gestión de la vulnerabilidad técnica.		
	12.6.1	Control de las vulnerabilidades técnicas	No Aplica	N/A
			Efectividad conjunta:	**33%**
13. Gestión de incidentes de la seguridad de la Información	13.1	Reportando eventos y debilidades de la seguridad de la información.		30%
	13.1.1	Notificación de los eventos de seguridad de la información.	Reproducible, pero intuitivo	50%
	13.1.2	Notificación de puntos débiles de seguridad.	Inicial / Ad-hoc	10%
	13.2	Gestión de incidentes y mejoras de seguridad de la información.		23%
	13.2.1	Responsabilidades y procedimientos.	Inicial / Ad-hoc	10%
	13.2.2	Aprendizaje de los incidentes de seguridad de la información.	Inicial / Ad-hoc	10%
	13.2.3	Recopilación de evidencias.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**26%**

14. Gestión de la continuidad del negocio	14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.		8%
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Inicial / Ad-hoc	10%
	14.1.2	Continuidad del negocio y evaluación de riesgos.	Inexistente	0%
	14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	Inicial / Ad-hoc	10%
	14.1.4	Marco de referencia para la planificación de la continuidad del negocio.	Inicial / Ad-hoc	10%
	14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**8%**
15.Cumplimiento	15.1	Cumplimiento con los requisitos legales.		40%
	15.1.1	Identificación de la legislación aplicable.	Inexistente	0%
	15.1.2	Derechos de propiedad intelectual (DPI).	Reproducible, pero intuitivo	50%
	15.1.3	Protección de los documentos de la organización.	Reproducible, pero intuitivo	50%
	15.1.4	Protección de datos y privacidad de la información de carácter personal.	Reproducible, pero intuitivo	50%
	15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.	Reproducible, pero intuitivo	50%
	15.1.6	Regulación de los controles criptográficos.	No Aplica	N/A
	15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.		30%
	15.2.1	Cumplimiento de las políticas y normas de seguridad.	Reproducible, pero intuitivo	50%
	15.2.2	Comprobación del cumplimiento técnico.	Inicial / Ad-hoc	10%
	15.3	Consideraciones sobre las auditorías de los sistemas de información.		10%
	15.3.1	Controles de auditoría de los sistemas de información.	Inicial / Ad-hoc	10%
	15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**30%**