UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERIA EN COMPUTACIÓN E INFORMÁTICA

ESTÁNDAR INTERNACIONAL ISO 27001 PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA CENTRAL DE INFORMÁTICA DE LA UNPRG.

TESIS

PRESENTADO POR:

VICTOR EDUARDO ZEÑA ORTIZ

PARA OPTAR EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN E INFORMÁTICA

LAMBAYEQUE - PERÚ

2015

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

ESTÁNDAR INTERNACIONAL ISO 27001 PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA CENTRAL DE INFORMÁTICA DE LA UNPRG

TESIS

PRESENTADO POR:

VICTOR EDUARDO ZEÑA ORTIZ

PARA OPTAR EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN E INFORMÁTICA

LAMBAYEQUE - PERÚ

2015

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE COMPUTACIÓN E INFORMÁTICA

ESTÁNDAR INTERNACIONAL ISO 27001 PARA LA GESTIÓN DEL SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA CENTRAL DE INFORMÁTICA DE LA UNPRG

Tesis presentada a la Universidad Nacional Pedro Ruiz Gallo, para obtener el Título de: INGENIERO DE COMPUTACIÓN E INFORMÁTICA.

Victor Eduardo Zeña Ortiz
Bach. Computación e Informática

Ing. Denny John Fuentes Adrianzén
ASESOR

APROBADA POR HONORABLE JURADO:

Mg. Gilberto Carrión
PRESIDENTE

Ing. Alejandro Chayán Coloma
SECRETARIO

Ing. Percy Celis
Ing. VOCAL

LAMBAYEQUE – PERÚ – 2015

DEDICATORIA

Dedico este trabajo a mis amados padres Carlos y Fely, ya que gracias a ellos y a su apoyo integro he logrado alcanzar y cumplir cada una de mis metas trazadas. Ya que sin ustedes no lo hubiera logrado. Esto es para ustedes amados padres.

A mi hermano Carlos Javier Zeña, ya que gracias a él, a sus concejos y recomendaciones busqué ser como él. Gracias por compartir muy buenos y gratos momentos en mi vida.

A cada uno de mis amigos ya que fueron pieza fundamental en mi formación, por sus concejos y por compartir una linda amistad

AGRADECIMIENTO

A Dios, por todas las bendiciones recibidas y por siempre cuidar de mí y de cada una de las personas que amo.

Un agradecimiento especial al Ing. Carlos Rivera por su apoyo constante en esta investigación y a cada una de las personas que contribuyeron a la finalización de este trabajo de investigación.

Agradecer a la Universidad Nacional Pedro Ruiz Gallo por la formación académica que me ha brindado.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El objetivo principal de este trabajo de investigación es la aplicación del Estándar Internacional ISO 27001 en el Análisis y Evaluación en la gestión de seguridad de la información para el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG. Teniendo como población todos los activos de información que intervienen en el servicio de Soporte de TI.

La recolección de la información e identificación de activos se realizó mediante observación y reuniones con el personal clave de cada sub proceso, utilizando para su elaboración la Metodología Magerit III conjuntamente con la ISO 27001 para el análisis y evaluación de riesgos del sistema de gestión de seguridad de información por ser la más acorde y utilizada en diferentes organizaciones ya sean públicas o privadas.

La implementación del Sistema de Gestión de Seguridad de la Información en el proceso de Soporte de TI redujo el nivel de riesgo en un 26.67%, los controles aplicados se incrementaron en un 44.88 % y se mejoró las opciones de Tratamiento en un 46.67%, mejorando de esta manera el proceso de Soporte de TI de la Oficina Central de Informática.

En conclusión este Sistema de Gestión de Seguridad de la Información mejoró en gran medida el proceso de Soporte de TI con respecto a la disminución del nivel de riesgo, incremento de los controles aplicados y mejora de las opciones de tratamiento en la oficina central de informática.

PALABRAS CLAVES:

ESTÁNDAR INTERNACIONAL ISO 27001 – SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SEGURIDAD DE INFORMACIÓN – SGSI

ABSTRACT

The main objective of this research is the application of International Standard ISO 27001 in the analysis and evaluation in the management of information security to the process of IT Support Office in the Central Informatics UNPRG. Taking as population all information assets involved in IT service support.

The data collection and identification of assets held by observation and meetings with key staff of each sub process for processing using the Magerit III Methodology conjunction with ISO 27001 for analysis and risk assessment of the safety management system Information to be the most consistent and used in different organizations whether public or private.

Implementation of Safety Management System Information in the process of IT support reduced the level of risk by 26.67%, the controls applied increased by 44.88% and treatment options are improved by 46.67%, improving thus the process of IT support of the Central Office of Information.

In conclusion this Management System Information Security greatly improved the process of IT support with regard to decreasing the level of risk, increased inspection procedures and improved treatment options in the central informatics.

KEYWORDS:

INTERNATIONAL STANDARD ISO 27001 - MANAGEMENT SYSTEM INFORMATION SECURITY - SAFETY INFORMATION - ISMS

CAPÍTULO I
MARCO LÓGICO

1.1. Realidad Problemática

En la actualidad, las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionajes, sabotajes, vandalismos, incendios o inundaciones; también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Es por esto, que enfocando el presente proyecto en la realidad peruana y específicamente en el contexto de la región de Lambayeque, se creyó conveniente traer a la memoria algunas empresas del medio que cuentan con un Sistema de Gestión de la Seguridad de la Información como: Mi Banco, Telefónica y Nextel S.A; empresas que enfrentan serios problemas de seguridad en la información, que rara vez se centran en aspectos de carácter técnico exclusivamente, sino de gestión, es decir de cómo alinear la tecnología con los objetivos de la organización.

Si se tiene en cuenta que la información adopta diversas formas, ya que, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o expresada oralmente en conversación; sea cual sea la forma en la que se muestre, comparta o almacene, necesita protegerse adecuadamente; ante esto, se optó por la aplicación del Estándar Internacional ISO 27001, en el ámbito informático de la Universidad Nacional Pedro Ruiz Gallo, delimitando su alcance en el área de Soporte de TI de la Oficina Central de Informática; con lo cual se pretende garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados; de manera que se busque proteger la información de la gran amplitud de rango de amenazas a que está expuesta.

1.2. Formulación del problema científico

¿De qué manera la aplicación del Estándar Internacional ISO 27001 mejora la Gestión de Seguridad de la Información en el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG?

1.3. Hipótesis

1.3.1. Hipótesis General

Si se aplica el Estándar Internacional ISO 27001 mejora de manera eficaz y eficiente la Gestión de Seguridad de la Información en la Oficina Central de Informática de la Universidad Nacional Pedro Ruiz Gallo.

1.4. Objetivos

1.4.1. Objetivo General

Aplicar el Estándar Internacional ISO 27001 para la Gestión de Seguridad de la Información en el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG.

1.4.2. Objetivos Específicos

- Determinar la influencia de la aplicación del Estándar Internacional ISO 27001 en el Análisis y Evaluación en la gestión de seguridad de la información para el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG.

- Disminuir el Nivel de Riesgos de Seguridad en el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG.

- Incrementar los Controles de Seguridad en el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG.

- Determinar la influencia de la aplicación de Estándar Internacional ISO 27001 en las Opciones de tratamiento de riesgos en el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG.

- Disminuir el Riesgo de Pérdidas Económicas en el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG.

1.5. Justificación e Importancia

Desde el punto institucional, la Universidad Nacional Pedro Ruiz Gallo para obtener una ventaja competitiva dentro de las otras Universidades, debe garantizar la seguridad de la información en cada uno de los procesos de las diferentes áreas. Esto permitirá encaminar a la Universidad a la Certificación ISO 27001. Brindando seguridad a los alumnos, docentes y administrativos, buscando contribuir con el crecimiento institucional, según ISO 27001, esta norma cubre todo tipo de organizaciones (por ejemplo, empresas comerciales, instituciones gubernamentales, organizaciones sin fines de lucro)

Desde el punto de vista económico, un Sistema de Gestión de Seguridad de Información permite reducir costos significativamente; además, instrumentos de control riesgos económicos, de gasto, verificaciones sobre la implementación de las actividades, elegibilidad de los gastos, archivo y conservación de la documentación, permitiendo incrementar las ganancias y estar al alcance tecnológico de las diversas entidades educativas de nivel superior. Por la ineficacia y la ineficiencia de los sistemas de gestión de seguridad de información las pérdidas son millonarias (Alexander, 2007).

Desde el punto de vista operacional, debido a la existencia de la problemática mencionada, es necesaria su implementación para mejorar la seguridad y calidad del servicio a estudiantes, docentes y administrativos, otorgándole a la Universidad el valor agregado de una Certificación ISO 27001 que necesita para fortalecerse frente a sus competidores directos como son las diferentes entidades educativas en la región.

Esta norma adopta un enfoque basado en procesos para poder mejorar el SGSI de una organización. Cualquier actividad que utiliza recursos y que se gestiona para permitir que los elementos de entrada se transformen en resultados se puede considerar como un proceso. (Alexander, 2007)

Desde el punto de vista tecnológico, se justifica debido a que los tiempos van cambiando y aparecen nuevas exigencias y las organizaciones deben adaptarse a estos cambios, de tal manera que les permita desarrollarse adecuadamente.

Por lo tanto, a través de esta investigación se observa que mejorar un buen servicio seguro y de calidad de acuerdo a las exigencias de los estándares internacionales, permite garantizar un adecuado control de los riesgos de los procesos en la Universidad Nacional Pedro Ruiz Gallo. Según la ISO 27001, la ISO (Organización Internacional de Estandarización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial.

1.6. Antecedentes de la Investigación

a) Antecedente

Antecedente 1

Nacionales

Montoya, L. y López, M. (2011), en la tesis presentada a la Universidad Nacional Mayor de San Marcos, acerca del Diseño de una Metodología de Gestión de Riesgos de Seguridad de la Información para Entidades Financieras, analizaron la problemática basada en el crecimiento acelerado de los mercados financieros y la evolución de la bancarización, significando que los ciudadanos acudan a las instituciones financieras en busca de un servicio de ahorro para sus recursos financieros y en la oportunidad de poder acceder a un crédito en forma oportuna y eficaz. Dicho crecimiento financiero ha generado también un uso creciente de tecnologías de información y comunicaciones, su objetivo es involucrar a la Alta Dirección y el compromiso de todos los miembros de la organización, hacia una cultura de control interno y prevención del riesgo, basado en los diferentes lineamientos, marcos de referencia, estándares y regulaciones vigentes, adaptado a las necesidades y requerimientos de cada Entidad, buscando la seguridad de la información y la continuidad del negocio; de tal manera, que se agregue valor y ventaja competitiva a las operaciones que realizan. Para así tener como resultado diseñar una metodología de gestión de riesgos de seguridad de la información que busque proteger los activos de información de la organización tomando como referencia los lineamientos y principios de ISO 27002:2005, COSO-ERM, y MAGERIT v3.0. Finalmente se desarrolla, se seleccionan e

implementan controles que minimicen el riesgo y contribuyan a garantizar la seguridad de los activos de información.

La conclusión más importante de los autores indicó lo siguiente:

La protección de la información se ha convertido en un tema de gran trascendencia, habiendo pasado a ocupar un lugar prioritario en las agendas de los reguladores, de los supervisores, de las entidades, de los investigadores y de todos los interesados en el sector financiero, puesto que garantiza su competencia en el mercado y el desarrollo exitoso del negocio.

Esta conclusión resultó importante porque coincide con una de las variables de estudio del presente trabajo, ya que la problemática basada en el crecimiento acelerado de los mercados financieros y la evolución de la bancarización, ha significado que los ciudadanos acudan a las instituciones financieras en busca de un servicio de ahorro para sus recursos financieros y en la oportunidad de poder acceder a un crédito en forma oportuna y eficaz. De este antecedente se ha tomado la importancia de asegurar la información en una organización, ya que se constituye en un gran potencial inmerso en ella.

Antecedente 2

Ampuero, C. (2011), en la tesis presentada a la Pontificia Universidad Católica del Perú, presentó un Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de seguros, afirmando que en la actualidad, con el desarrollo de la tecnología, la información ha tomado mayor fuerza en las empresas, convirtiéndose en la mayoría de los casos en el activo más importante que tienen.

Es por esta razón que tienen la obligación de proteger aquella información que es importante para ellas y que tiene relación ya sea con el negocio o con los clientes. La Superintendencia de Banca, Seguros y AFP, en el 2009, elaboró la circular G140, que estipula que todas las empresas peruanas que son reguladas por este organismo deben contar con un plan de seguridad de información. La presente tesis tiene como objetivo diseñar un sistema de gestión de seguridad de información para una compañía de seguros que cubra lo que pide la circular para evitar problemas regulatorios con este organismo. Para esto, se utilizan estándares y buenas prácticas, reconocidos mundialmente, cabe resaltar que estos estándares y buenas prácticas indican qué es lo que se debe realizar, pero no especifican cómo se deben implementar los controles. Estos van a depender de la necesidad de la empresa y de la inversión que desee realizar en temas de seguridad, con lo que se puede afirmar que lo expuesto en la tesis es una forma de cómo se puede diseñar un Sistema de Gestión de Seguridad de Información. En conclusión actualmente se vive en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de compañías, convirtiéndose así en su activo más importante. Por ejemplo, si en algún momento se da un terremoto; en cambio, si llegamos a perder la información de la compañía, es muy probable que no se pueda recuperarla si no se tienen las consideraciones debidas, con lo que es probable que la empresa deje de operar. Partiendo de esta premisa, es importante contar con un Sistema de Gestión de Seguridad de la Información para poder asegurar, a un nivel aceptable, la información de la compañía.

El aporte de este antecedente es que coincide con el presente trabajo ya que busca diseñar un sistema de gestión de seguridad de información para dar cumplimiento a lo estipulado en la circular, así

como para evitar problemas regulatorios con este organismo. Para esto, se utilizan estándares y buenas prácticas reconocidos mundialmente para poder desarrollar cada una de las etapas del diseño del Sistema de Gestión de Seguridad de Información (SGSI) y así poder tener una base que se pueda implementar en cualquier organización empresarial o educativa. De este antecedente se han tomado el uso de los estándares y buenas prácticas reconocidas mundialmente, para de esta manera proteger la información.

Antecedente 3

Internacionales

Lara, H., Reyes, J. y Navarrete, W. (2006), en su tesis para optar el título profesional en la Escuela Superior Politécnica del Litoral, Ecuador, presentó una tesis referida al diseño de sistema de gestión de seguridad de información para ECUACOLOR, La empresa Ecuacolor se dedica en la actualidad a la captura, reproducción, conservación y comunicación de imágenes que son los más preciados recuerdos y sentimientos del ser humano. Gracias a la utilización de tecnología de punta a la experiencia de su recurso humano y a la capacitación continua, ha logrado colocarse como líder en la comercialización y distribución de productos y servicios fotográficos, uno de los problemas que presenta dicha empresa es que las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. Los hackers que son expertos en Ingeniería Social, consiguen personas dentro de la compañía para sacarles contraseñas y claves de invitados, estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad. El objetivo de esta tesis es implementar un Sistema de Gestión de Seguridad de la Información

para la empresa Ecuacolor, basado en el análisis de la empresa y el conocimiento adquirido durante el Diplomado de Auditoría Informática de esta manera contribuir para que las empresas ecuatorianas tomen conciencia de la necesidad de implementar Sistemas de Seguridad, como una herramienta que ayudará a cumplir con las metas y objetivos de la empresas, ayudándoles en la gestión del negocio y ser más competitivas en el mercado. En conclusión, se establece una cultura de seguridad y una excelencia en el tratamiento de la información en todos sus procesos de negocio. Así, aporta un valor añadido de reconocido prestigio, en la calidad de los servicios que ofrece a sus clientes.

Este antecedente coincide con las variables del presente estudio, y advierte acerca del papel de los hackers, que son expertos en Ingeniería Social. Esas personas dentro de la compañía consiguen extraer contraseñas y claves de invitados; estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de gestionar la seguridad. De este antecedente se ha tomado la importancia de realizar una buena gestión de seguridad de la información.

Antecedente 4

Pallas, G. (2009), presentó una tesis en la Universidad de la República de Uruguay, donde enfocó la Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. La problemática se plantea de la siguiente manera, es un hecho que los sistemas de gestión y de información están muy arraigados en los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. Esta dependencia de los sistemas de información en general, justifica el dotar de seguridad a

los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de sus activos. Ya no es suficiente con establecer controles en forma aislada ni ad hoc, tampoco es suficiente actuar de modo meramente reactivo y defensivo, cuyo objetivo es el de implementar un sistema de gestión de seguridad de la información (SGSI) y así tener un accionar proactivo. Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos (serie ISO/IEC 27.000), y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información (por ejemplo ISM3). Se promueve un enfoque sistémico y pragmático, no dogmático, en pro de una metodología eficaz y sostenible, primando un criterio de conveniencia costo-beneficio. Se presenta una metodología adecuada a un grupo empresarial, que busca integrar lo mejor de cada uno de los enfoques analizados; se incluye una propuesta de organigrama de Seguridad que compatibiliza la jerarquía estructural del grupo y las necesidades de un SGSI. Finalmente tenemos como resultado del estudio, los estándares y recomendaciones internacionales específicos, el modelo organizacional aplicable al negocio, datos estadísticos, y la seguridad requerida para este sector de la industria.

El antecedente es importante porque existen diferentes estándares que se desarrollan para gestionar la seguridad de la información, algunos más generales, otros centrados en la gestión de riesgos (serie ISO/IEC 27.000), incluso aquellos tendientes a desarrollar un modelo de madurez de la seguridad de la información (por ejemplo, ISM3).

En la tesis consultada se analizan diferentes métodos de análisis y gestión de riesgos. Algunos de ellos promovidos por los gobiernos y/o industrias de países de vanguardia y trayectoria reconocida en la

seguridad de la información que han tenido gran aceptación. Se promueve un enfoque sistémico y pragmático, no dogmático, en pro de una metodología eficaz y sostenible, primando un criterio de conveniencia costo-beneficio. Se presenta una metodología adecuada a un grupo empresarial, que busca integrar lo mejor de cada uno de los enfoques analizados; se incluye una propuesta de organigrama de Seguridad que compatibiliza la jerarquía estructural del grupo y las necesidades de un SGSI.

Adicionalmente se incursiona en la aplicación de técnicas de grafos para la valoración de activos; se formaliza el concepto en términos de propiedades y algoritmia de grafos, y se define con una visión propia del tema, un algoritmo para el ajuste contemplando valoraciones cualitativas y cuantitativas y dependencias parciales y/o totales entre activos. Finalmente se analiza la aplicación de la metodología a un Caso de Estudio, en particular, un 'Internet Service Provider' (ISP) integrado verticalmente con una 'TelCo' (empresa de Telecomunicaciones). En el mismo se analizan las particularidades del caso de estudio: los estándares y recomendaciones internacionales específicos, el modelo organizacional aplicable al negocio, datos estadísticos, y la seguridad requerida para este sector de la industria. De este antecedente se ha tomado, la implantación de un Sistema de Gestión de Seguridad de la Información y enfatiza la necesidad de su orientación y adecuación a los reales requerimientos de seguridad del negocio.

1.7. Definición de variables

1.7.1. Variable Independiente

- ✓ Estándar Internacional ISO 27001.

1.7.2. Variables Dependientes

- ✓ Sistema de Gestión de Seguridad de la Información.

1.7.3. Variable interviniente

1.7.3.1. Metodológica

- ✓ Modelo PDCA
  - Metodología análisis de riesgos MAGERIT.

1.7.3.2. Tecnología

- ✓ Computadoras.
- ✓ Internet.
- ✓ Foros Tecnológicos.

1.7.4. Herramientas

Las técnicas y herramientas utilizadas para desarrollar los sistemas de información, son: entrevistas, encuesta, cuestionario y observación.

1.8. Beneficios

1.8.1. La Empresa (Ejecutivos, Personal)

El Sistema de Gestión de Seguridad de la información ha sido diseñado con la finalidad de ser utilizado por los propietarios de los procesos del negocio, como guía clara y entendible, con el fin de alcanzar los objetivos trazados por la empresa.

1.8.2. Futuras Investigaciones

El presente trabajo de investigación sirve como aporte para otros estudios que tiendan a desarrollar trabajos relacionados con la seguridad de la información, pues el trabajo cuenta con una sólida base científica con respecto a lo que en seguridad se refiere.

1.8.3. En lo Social

El Diseño de Gestión de Seguridad de la Información permite a las organizaciones tener una mejor apreciación y entendimiento de los riesgos y limitaciones de TI, a todos los niveles dentro de la empresa con el fin de obtener una efectiva dirección y controles, de manera tal, maximizar sus beneficios, capitalizar sus oportunidades y ganar ventaja competitiva.

1.8.4. En lo Personal.

Se logra adquirir nuevos conocimientos ante las posibilidades de conocer sobre seguridad de la información la cual permite fijar los mecanismos y procedimientos que deben adaptar las empresas para salvaguardar los sistemas y la información que estas contienen.

CAPÍTULO II
MARCO REFERENCIAL

2.1. Marco teórico

2.1.1. Sistema de Gestión de Seguridad de la Información

2.1.1.1. Definiciones

El Sistema de gestión de seguridad de la información permite tener una mejor administración de los activos de la empresa. Areitio, J. (2008), indica que permite asegurar la aptitud de un sistema de información en base a la disuasión, protección, detección, respuesta y capacidad de recuperación, proporcionando las garantías de sus activos en base a la confidencialidad, la integridad, la disponibilidad, la responsabilidad, la autenticidad y la fiabilidad, teniendo en cuenta las amenazas percibidas.

Además permite ir de la mano con la gerencia, para asimismo tener un compromiso por parte de ella. Alexander, A. (2007), indica que es parte del sistema de gestión global, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar la seguridad de la información.

ISO 27001, (2005) indica de que un Sistema de Gestión de Seguridad de la Información debe estar formado por lo siguiente:

- **Alcance del Sistema de Gestión de Seguridad de la Información:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información 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 Sistema de Gestión de Seguridad de la Información considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- **Identificación de activos:** Acá se procede a identificar todos los diferentes activos que presenta la entidad.

- **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.

- **Enfoque de evaluación de riesgos:** Descripción de la metodología a emplear (cómo se realiza 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.

- **Análisis y evaluación:** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

- **Opciones de Tratamiento:** Una vez efectuado el análisis y evaluación del riesgo, se debe decidir cómo tratar el riesgo basándose en las siguientes opciones:

  - ✓ **Reducir:** Establecer controles para atenuación (políticas, procedimientos, procesos y herramientas).

- ✓ **Aceptar:** Aceptar el riesgo en su presente nivel debido a que no es posible realizar un tratamiento o porque éste resulta demasiado caro.

- ✓ **Transferir:** Transferir a un tercero con capacidad financiera / especialización necesaria para administrar el riesgo adecuadamente.

- ✓ **Evitar:** Evitar el riesgo eliminándolo de la actividad de la organización.

- **Enunciado de aplicabilidad:** documento que contiene los objetivos de control y los controles contemplados por el Sistema de Gestión de Seguridad de la Información, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

- **Plan de tratamiento de riesgos:** documento que identifica las acciones de la dirección, recursos, responsabilidades y 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.

2.1.1.2. Importancia de la gestión de riesgos de seguridad de la información para la entidad

- Reduce los riesgos, amenazas y vulnerabilidades que afectan a los activos de información de la institución.

- Garantiza la confidencialidad, integridad y disponibilidad de la información

- Busca lograr la confiabilidad en la información de la Oficina Central de Informática.

- Previene riesgos y gestiona incidentes de seguridad de información.

- Fomenta la cultura de seguridad de información en la Oficina Central de Informática.

- Protege la información contra los riesgos de destrucción, pérdida, divulgación, malversación y no disponibilidad.

2.1.2. Seguridad de Información

2.1.2.1. Definiciones

La seguridad de la información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. (ISO/IEC 17799, 2005). Así pues, estos tres términos (Figura N° 1) constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** La información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

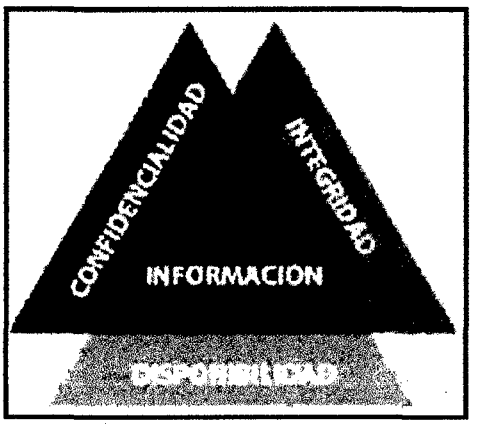


Figura N° 1: La base para la seguridad de información

Fuente: Elaboración Propia

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información.

2.1.3. Estándar Internacional ISO 27001

2.1.3.1. Definiciones

ISO 27001, (2005), este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un Sistema de Gestión de Seguridad de la Información debe ser una decisión estratégica para una organización. El diseño e implementación del mismo en una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Este Estándar Internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

Calder, A. (2006), indica que este es el más reciente, más moderna y actualizada versión internacional de una especificación estándar para un sistema de gestión de seguridad de información. Independiente del proveedor y la tecnología. Está diseñado para su uso en organizaciones de todos los tamaños (con intención de ser aplicable a todas las organizaciones, independientemente de los tipos, tamaño y naturaleza) y en todos los sectores en cualquier parte del mundo.

FASES DEL ISO 27001: Según ISO 27001, (2005) indica que la ISO cumple con las siguiente fases (Figura N° 2):

- ✓ **P (Plan):** A través del cual se establece el SGSI
- ✓ **D (Do):** A través del cual se implementa y opera el SGSI
- ✓ **C (Check):** A través del cual se monitorea y revisa el SGSI
- ✓ **A (Act):** A través del cual se mantiene y mejora el SGSI

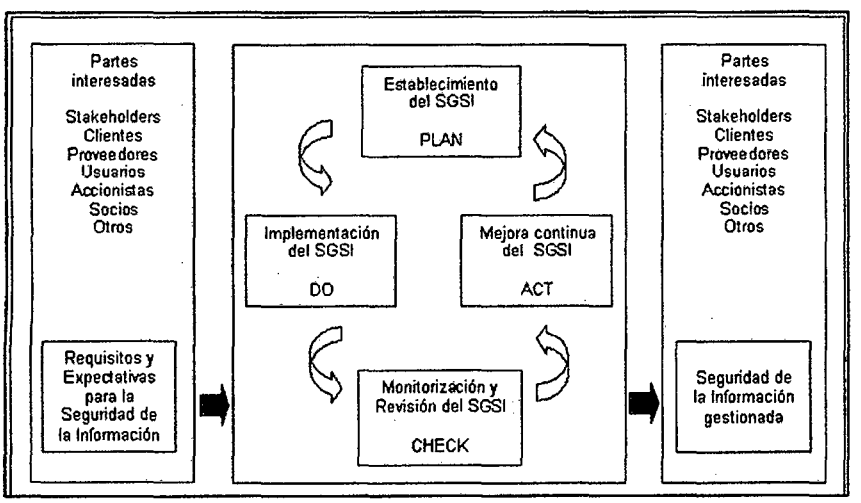


Figura N° 2 Modelo del desarrollo del SGSI

Fuente: ISO 27001

En la primera fase, **"Establecimiento del SGSI"**, se dan las pautas para determinar el alcance del modelo del SGSI, identificar los activos de información y tasarlos, luego hacer el análisis y la evaluación del riesgo y determinar que activos de información están sujetos a riesgo. Seguidamente, en esta fase se determinan las opciones para el tratamiento del riesgo.

En la segunda fase, **"Implementación del SGSI"**, se elabora el plan de tratamiento del riesgo, detallando las acciones que deben emprenderse para implementar las opciones de tratamiento del riesgo escogidas.

En la tercera fase, **"Monitoreo y Revisión"**, se establecen procedimientos y rutinas establecidos, con ayuda de métrica, revisar el desempeño del SGSI.

En la cuarta fase, **"Mejora continua"**, se toman las acciones pertinentes para reaccionar a incidentes y tomar también las acciones preventivas de lugar. La idea consiste en llevar al SGSI a la excelencia en el tiempo

2.1.4. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

El análisis de riesgo es un elemento imprescindible en la implementación del Sistema de Gestión de Seguridad de la Información para el Servicio de Soporte de TI, además de ser un requerimiento de la ISO 27001, permitiendo identificar los riesgos que deben ser gestionados de manera más inmediata. El modelo de administración de riesgos de seguridad de información consta de un proceso continuo de 4 fases principales que permite medir y manejar los riesgos de seguridad de información en un nivel aceptable. La

presente metodología está basado Magerit v3.0, y en el estándar ISO 27001:2005.

La metodología de Gestión del Riesgo se ha dividido en 4 partes:

I. Inventario de Activos de Información

II. Análisis del Riesgo

III. Evaluación del Riesgo

IV. Tratamiento del Riesgo

El siguiente Figura muestra el flujo de actividades de la metodología (Figura Nº 3):

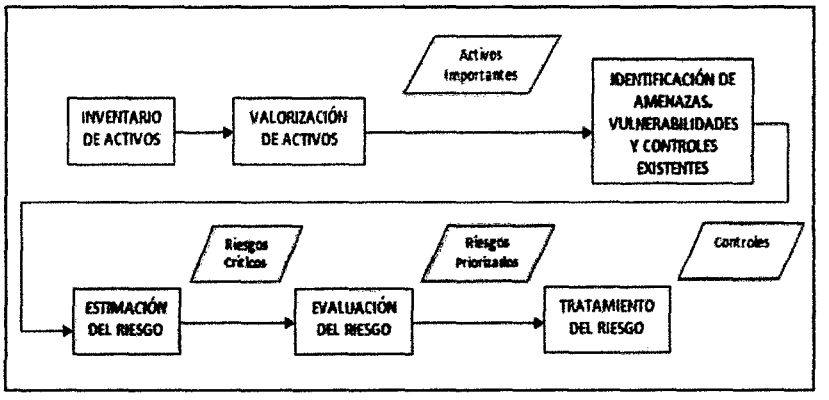


Figura N° 3 Metodología del Análisis, Evaluación y Tratamiento del Riesgo

Fuente: Elaboración propia.

2.1.5. Inventario de activos de información

Inventario de Activos

Los activos de información en la organización, dentro del alcance del Sistema de Gestión de Seguridad de la Información, son fundamentales para una correcta implementación de un Sistema de Gestión de Seguridad de la Información.

Los activos importantes deben ser identificados y posteriormente tasados por un grupo multidisciplinario compuesto por personas (generalmente los propietarios) involucradas en los procesos y subprocesos que abarca el alcance del Sistema de Gestión de Seguridad de la Información.

Por cada activo se deben definir:

- Código
- Nombre
- Tipo
- Propietario
- Proceso al que pertenece

Valorización de Activos

La valorización es la importancia del activo de información para la organización, en cuanto a su Confidencialidad, Integridad y Disponibilidad (CID). Los valores de importancia están en una escala penta:

Escala	Valor de Importancia	Descripción
1	MUY BAJO	Nivel de criticidad del activo es muy bajo.
2	BAJO	Nivel de criticidad del activo es bajo.
3	MEDIO	Nivel de criticidad del activo es medio.
4	ALTO	Nivel de criticidad del activo es alto.
5	MUY ALTO	Nivel de criticidad del activo es muy alto.

Tabla 1: Valoración del Activo

Fuente: Elaboración propia

Cada proceso dentro de su contexto, el significado de la importancia alta, media o baja del activo. El Valor del Activo resulta del promedio (redondeado hacia arriba) de los valores CID obtenidos. A continuación se presentan unos ejemplos:

Nombre del Activo	Clasificación	Tipo	Propietario	Importancia del activo			
				C	I	D	TOTAL
Informe 1	Confidencial	Información	X	5	5	4	5
Reporte 2.xls	Restringido	Información	X	4	4	3	4
PC 1		Hardware	Y	-	-	4	4
Personal X		Personal		-	-	3	3

Tabla 2: Ejemplo de Valorización del Activo

Fuente: Elaboración propia

Los activos cuyo Valor del Activo (promedio) sea Alto (4) o Muy Alto (5) pasan a la fase de Análisis de Riesgos.

2.1.6. Análisis de Riesgos

2.1.6.1. Identificación de las Amenazas, Vulnerabilidades y Controles Existentes

1. Amenazas

Los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y sus activos.

Las amenazas han sido clasificadas de acuerdo a su naturaleza, para facilitar su ubicación, como se muestra en la siguiente tabla (Anexo N° 07):

Las amenazas se pueden originar de fuentes o eventos accidentales o deliberados. Para que una amenaza cause daño tendrá que explotar una o más vulnerabilidades de los activos de la organización.

2. Vulnerabilidades

Las vulnerabilidades no causan daño, simplemente son condiciones que pueden hacer que una amenaza se materialice y afecte a un activo. Las vulnerabilidades han sido clasificadas, como se muestra en la siguiente tabla (Anexo N° 8):

Las vulnerabilidades y las amenazas deben presentarse juntas para poder causar incidentes que pudiesen dañar los activos. Por esta razón es necesario entender la relación entre amenazas y vulnerabilidades.

Las variables que la organización puede manipular para minimizar el riesgo y proteger los activos de la materialización de una amenaza, son las vulnerabilidades.

3. Controles Existentes

Los controles, que contrarrestan la materialización de una amenaza ya aplicados por la organización, deben ser identificados, para poder medir su eficacia. Un control ineficaz es una vulnerabilidad.

2.1.6.2. Determinación del valor de Degradación

La degradación es el grado en que se ve afectado el activo de información, cuando una vulnerabilidad es explotada por una amenaza. Se valoriza la degradación considerando las vulnerabilidades y controles existentes, en cuanto a las dimensiones de Confidencialidad, Integridad y Disponibilidad (CID). Los valores de degradación están en una escala penta:

Escala	Valor de Importancia	Descripción
1	MUY BAJO	Nivel de degradación del activo es muy bajo.
2	BAJO	Nivel de degradación del activo es bajo.
3	MEDIO	Nivel de degradación del activo es medio.
4	ALTO	Nivel de degradación del activo es alto.
5	MUY ALTO	Nivel de degradación del activo es muy alto.

Tabla 3: Determinación del Valor de Degradación

Fuente: Elaboración propia

El Valor de la Degradación es el valor máximo de las 3 degradaciones CID obtenidas.

2.1.6.3. Determinación del valor de Impacto

El Impacto toma en cuenta la Degradación, así como el Valor del activo. La fórmula es la siguiente:

$$\text{IMPACTO} = (\text{Degradación}_{(\text{máx.})} + \text{Valor Activo})/2$$

Los valores del Impacto se redondean al valor entero más próximo, como se muestran en la siguiente escala:

Promedio Aritmético	Valor del Impacto	Significado
[1 - 1.4]	**1 (MB)**	MUY BAJO
[1.5 - 2.4]	**2 (B)**	BAJO
[2.5 - 3.4]	**3 (M)**	MEDIO
[3.5 - 4.4]	**4 (A)**	ALTO
[4.5 - 5]	**5 (MA)**	MUY ALTO

Tabla 4: Determinación del valor de impacto

Fuente: Elaboración propia

2.1.6.4. Determinación de la Probabilidad

La probabilidad es la posibilidad de que se materialice una amenaza, es decir, que se produzca un ataque exitoso de una amenaza, tomando en cuenta las vulnerabilidades y los controles existentes. Para el presente análisis se toman en cuenta los siguientes valores de probabilidad en una escala penta:

Escala	Valor de Importancia	Descripción
1	MUY BAJO	Nivel de probabilidad del activo es muy bajo.
2	BAJO	Nivel de probabilidad del activo es bajo.
3	MEDIO	Nivel de probabilidad del activo es medio.
4	ALTO	Nivel de probabilidad del activo es alto.
5	MUY ALTO	Nivel de probabilidad del activo es muy alto.

Tabla 5: Determinación de la Probabilidad

Fuente: Elaboración propia

2.1.6.5. Determinación del Riesgo

El riesgo es la combinación de la probabilidad de una amenaza se materialice y las consecuencias que acarrea dicho ataque (Impacto). La fórmula es la siguiente:

RIESGO = (Impacto + Probabilidad)/2

Los valores del Impacto se redondean al valor entero más próximo, como se muestra en la siguiente tabla:

MATRIZ RIESGO			IMPACTO				
			Muy Bajo	Bajo	Medio	Alto	Muy Alto
			1	2	3	4	5
PROBABILIDAD	Muy Bajo	1	1	2	2	3	3
	Bajo	2	2	2	3	3	4
	Medio	3	2	3	3	4	4
	Alto	4	3	3	4	4	5
	Muy Alto	5	3	4	4	5	5

Tabla 6: Determinación del Riesgo

Fuente: Elaboración propia

2.1.6.6. Criterio de Aceptación del Riesgo

El criterio de aceptación del riesgo se detalla en la siguiente tabla:

ESCALA	VALOR DEL RIESGO	SIGNIFICADO
1	RIESGO MUY BAJO	Un riesgo es aceptable cuando el activo se encuentra expuesto a riesgos leves o
2	RIESGO BAJO	

3	RIESGO MEDIO	moderados, por lo que NO amerita que sean tratados.
4	RIESGO ALTO	El activo se encuentra expuesto a riesgos altos o críticos y necesita ser tratado.
5	RIESGO MUY ALTO	

Tabla 7: Criterio de Aceptación del Riesgo

Fuente: Elaboración propia

Los Riesgos Altos (4) y Muy Altos (5) pasan a la fase de Evaluación del Riesgo.

Activo	Amenaza	Vulnerabilidad	Control Existente	Degradación			Degrad. Máx.	Valor Activo	Impacto	Probabilidad	RIESGO
				C	I	D					
Informe1	Robo			4	-	3	4	4	4	1	3
Informe1	Adulteración de activos			-	4	-	4	5	5	4	5
Reporte1.xls	Código malicioso			3	1	1	3	5	4	4	4

Tabla 8: Ejemplo de Criterio de Aceptación del Riesgo

Fuente: Elaboración propia

2.1.7. Evaluación del Riesgo

Luego de efectuado el cálculo del valor del riesgo, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos desde el punto de vista de la organización, para poder jerarquizarlos por su importancia.

A continuación se muestran los Criterios para la Evaluación del Riesgo que van a ser utilizados por la organización para evaluar la importancia del riesgo:

Criterios	Descripción
ECONÓMICO	Cuando el impacto económico de la amenaza es mayor a un porcentaje del costo mensual del servicio, o a un número determinado de U.I.T.
CONTINUIDAD	Cuando se paraliza un proceso de línea o al menos una actividad importante del mismo.
LEGAL	Aplica cuando el impacto ocasiona una demanda de índole civil o una denuncia de índole penal al proveedor, al Hospital o personal de una de ellas, lo cual ocasionaría la aplicación de una sanción y/o una indemnización en la vía civil o reparación en la vía penal.
IMAGEN	Cuando la amenaza puede ocasionar que se vea afectada la imagen de la institución y/o proveedores ante terceros (pensionistas, solicitantes, público en general).
CONTRACTUAL	Cuando el impacto amenaza el cumplimiento de contrato, debido a causas previsibles o no, siempre que se hallen determinados en el contrato.

Tabla 9: Evaluación del Riesgo

Fuente: Elaboración propia

A modo de ejemplo, se muestran algunas amenazas a las cuales se les ha realizado la evaluación del riesgo. El valor total resulta de la combinación del valor del riesgo con la cantidad de criterios aplicables. Luego se procede a ordenar los riesgos dándoles un orden de prioridad.

ANÁLISIS DEL RIESGO			EVALUACIÓN DEL RIESGO						
Activo	Amenaza	RIESGO	Económico	Continuidad	Legal	Imagen	Contractual	Subtotal	TOTAL
Informe 1	Robo	4		X			X	2	8
Informe 1	Adulteración de activos	5	X		X	X		3	15
Reporte 1.xls	Código malicioso	4				X		1	4

Tabla 10: Ejemplo de la Evaluación del Riesgo

Fuente: Elaboración propia

La evaluación del riesgo sirve para darle significancia e identificar los riesgos que requieren la aplicación priorizada de controles para su mitigación en la etapa de tratamiento del riesgo, o decidir que ciertos niveles de riesgo pueden ser aceptables, y que por tanto no requieren mayor acción.

2.1.8. Tratamiento de Riesgos

Opciones para el tratamiento del riesgo

Una vez efectuado el análisis y evaluación del riesgo, se debe decidir cómo tratar el riesgo basándose en las opciones, detalladas en la siguiente tabla:

Tratamiento	Descripción
Reducir	Establecer controles para atenuación (políticas, procedimientos, procesos y herramientas).
Aceptar	Aceptar el riesgo en su presente nivel debido a que no es posible realizar un tratamiento o porque éste resulta demasiado caro.
Transferir	Transferir a un tercero con capacidad financiera / especialización necesaria para administrar el riesgo

	adecuadamente.
Evitar	Evitar el riesgo eliminándolo de la actividad de la organización.

Tabla 11: Tratamiento de Riesgos

Fuente: Elaboración propia

Reducción del riesgo mediante aplicación de controles

En caso se haya seleccionado la alternativa de reducir el riesgo, se debe realizar las siguientes tareas:

- Identifica los controles implantados o existentes.
- Determina los nuevos controles a implementar para reducir el riesgo a un nivel aceptable.
- Implementación de controles

Aceptación de riesgo

En caso se haya seleccionado la alternativa de aceptar el riesgo, dicha aceptación debe ser incluida en la Declaración de Aplicabilidad de Riesgos y en el manual de evaluación y tratamiento de riesgo.

Evitar el Riesgo

En caso se haya seleccionado la alternativa de evitar el riesgo, se realiza las siguientes tareas:

- Identifica todos los elementos que se requiere para evitar que el riesgo se presente. Esto incluye los siguientes elementos: el activo y las amenazas relacionadas al activo.

- Se pide la aprobación de la gerencia para proceder a eliminar todos los elementos identificados en el acápite anterior.

- Se procede a eliminar todos los elementos identificados y aprobados por la gerencia, para tal fin aplicará un plan de acción que debe estar registrado en el documento de Gestión de riesgos del Sistema de Gestión de Seguridad de la Información y en el plan de tratamiento de riesgos.

Transferir el Riesgo

En caso se haya seleccionado la alternativa de transferir el riesgo, el Área Legal de la empresa, en conjunto con los encargados del Análisis y Evaluación de Riesgos del Sistema de Gestión de Seguridad de la Información realizan las siguientes tareas:

- Determinar la empresa o entidad que cubrirá el riesgo.

- Solicitar la aprobación de la gerencia para establecer un contrato con la empresa elegida.

- Incluir la transferencia del riesgo en el documento de Gestión de riesgos o el que haga sus veces.

Selección de controles para el tratamiento de riesgos

Los objetivos de control deben ser seleccionados e implementados para atender las necesidades identificadas en la evaluación de los riesgos y en el proceso de tratamiento de los riesgos.

Los objetivos de control serán seleccionados a partir del anexo A de la norma ISO/IEC 27001:2005.

La selección de los controles ha sido realizada con base en la evaluación de riesgos y los criterios para la definición de los niveles de aceptación y tolerancia al riesgo. Los detalles de la selección de controles se elaboraran en el documento **"Declaración de Aplicabilidad"**.

Declaración de Aplicabilidad

Se elabora la Lista de controles Aplicables y no Aplicables al Sistema de Gestión de Seguridad de la Información donde se detallan los controles seleccionados para poder cubrir los riesgos que superan el nivel de aceptación definido. Para esta selección se toma como base al Anexo A del estándar ISO/IEC 27001:2005.

Esto permite establecer mejoras a la gestión de la seguridad del proceso de Soporte de TI y facilita el proceso de implementación de las mismas.

GESTIÓN DE TRATAMIENTO DE LOS RIESGOS

1- Establecer el tratamiento del riesgo

La Alta Dirección conjuntamente con el equipo encargado de la evaluación y tratamiento del riesgo del Sistema de Gestión de Seguridad de la Información debe iniciar un proceso de toma de decisiones con respecto a cómo se trata el riesgo, de acuerdo a las opciones definidas anteriormente.

Las personas involucradas en la toma de decisiones, sobre el tratamiento del riesgo, deben analizar con cuidado la precisión y confiabilidad de la información, en las cuales basan su decisión y también visualizar el grado de pérdida que está dispuesto a aceptar.

2- Nivel de Aceptación y tolerancia al riesgo

El nivel de tolerancia al riesgo, también llamado en administración de riesgos como "apetito por el riesgo", es el elemento que fija la posición de una organización con respecto al nivel de riesgo que está dispuesta a afrontar como parte de las operaciones diarias en condiciones normales.

Para el presente Sistema de Gestión de Seguridad de la Información del proceso se ha definido seleccionar todos aquellos riesgos cuyo resultado sea mayor o igual a 4, priorizando de esta manera la mitigación de los riesgos encontrados en el análisis de riesgos.

3- Plan de Tratamiento del riesgo

Para la elaboración del plan de tratamiento de riesgos se ha determinado implementar controles que mitiguen los riesgos altos y muy altos tal.

Así mismo como primera implementación del Sistema de Gestión de Seguridad de la Información se considera disminuir los riesgos considerados como Altos y Muy Altos, en una próxima implementación se consideran los riesgos no tratados en esta oportunidad definiendo de esta manera el nivel de madurez del Sistema de Gestión de Seguridad de la Información en el proceso de Soporte de TI.

Es necesario indicar que la implementación de controles generales o específicos de implementación inminente no solo mitiga los riesgos identificados sino otros que no están contemplados para su tratamiento.

El desarrollo del Plan de Tratamiento de riesgos se elabora en el documento **"Plan de tratamiento de riesgos del sistema de gestión de seguridad de información".**

2.2. Marco Conceptual

Gestión de Seguridad de la Información: Asegura la aptitud de un sistema de información en base a la disuasión, la protección, la detección, la respuesta y la capacidad de recuperación, proporcionando las garantías de sus activos en base a la confidencialidad, la integridad, la disponibilidad, la responsabilidad, la autenticidad y la fiabilidad, teniendo en cuenta las amenazas percibidas. (Areitio, 2008).

Estándar Internacional ISO 27001: ISO (la Organización Internacional de Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial. Los organismos internacionales miembros de ISO e IEC participan en el desarrollo de Estándares Internacionales a través de los comités establecidos por la organización respectiva para lidiar con Áreas particulares de la actividad técnica. (ISO 27001, 2005).

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información, adicionalmente pueden involucrarse otras propiedades, tales como la autenticidad, responsabilidad, no repudio y confiabilidad. [ISO/IEC 17799:2005]

Activo: Factor dinámico que presenta valor para la organización [ISO/IEC 13335-1:2004]

Información: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente o hablada, actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia. [ISO/IEC 17799: 2005]

Riesgo: Se define como cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia. [AS/NZS 4360: 2004]

Control: Es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que

se realicen los ajustes o correcciones necesarias en caso se detecten eventos que escapan a la naturaleza del proceso. [ISO/IEC 17799:2005]

Es una etapa primordial en la administración, pues, por más que una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente, no se podrá verificar la situación real de la organización si no existe un mecanismo que verifique e informe si los hechos van de acuerdo con los objetivos.

Declaración de aplicabilidad: La declaración de aplicabilidad o SOA, del inglés Statement of Applicability, Es un documento que se referencia en la cláusula 4.2.1j del estándar ISO/IEC 27001 y describe los objetivos de control y controles relevantes y aplicables al alcance del SGSI de la empresa, en función de la política y conclusiones del proceso de evaluación y tratamiento del riesgo. En el documento básicamente van 2 campos: uno donde va el control específico y una columna donde va la aplicabilidad, donde se justifica la decisión tomada sobre si el control es aplicable o no. [ISO/IEC 27000:2005].

CAPÍTULO III
MARCO METODOLÓGICO

3.1. Hipótesis

La aplicación de un sistema de gestión de seguridad de la información ayuda a los responsables de la información a mejorar la seguridad de las tecnologías de información y comunicación.

3.2. Diseño de Contrastación de la Hipótesis

Se utiliza para la contratación de la hipótesis, el método de diseño en sucesión o en línea también llamado método Pre-Test, Post - Test, con un solo grupo.

El esquema es el siguiente:

$$O_1 \rightarrow X \rightarrow O_2$$

Figura N° 4: Diseño de contrastación de la hipótesis

Fuente: Elaboración Propia

O1: Análisis y la gestión de riesgos de un sistema de información antes del diseño del SGSI.

X : Diseño de un Sistema de Gestión de la Seguridad de la Información.

O2: Análisis y la gestión de riesgos de un sistema de información después del diseño del SGSI.

3.3. Tipo de Investigación

Tecnológica – Formal.

3.4. Población – Muestra

3.4.1. Población

"Es el conjunto de todos los elementos que forman parte del espacio territorial al que pertenece el problema de investigación y poseen características mucho más concretas que el universo" (Carrasco, 2006)

La población es el universo con el que se trabaja la tesis; se determina por la cantidad de Docentes y/o Administradores, Alumnos y Jefes y trabajadores de las áreas de estudio, responsables que acceden a manejos de información y que de una u otra manera contribuyen en el desarrollo de la tesis.

De acuerdo a la información proporcionada por la Oficina de Personal de la UNPRG, la población de estudio serán todos los usuarios beneficiarios de las diferentes dependencias de la universidad (en este caso el personal administrativo), que ascienden a un total de 762 trabajadores (entre 439 nombrados y 323 contratados).

3.4.2. Muestra

Es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llama población. (Hernández, 2007).

La muestra quedó determinada en 86 usuarios y se ha empleado la fórmula que aparece en el muestreo para su selección.

3.4.3. Muestreo

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1-p)}{(N-1) \cdot e^2 + Z^2 \cdot p \cdot (1-p)}$$

Figura N° 5: Diseño de contrastación de la hipótesis

Fuente: Elaboración Propia

La técnica a usada corresponde al muestreo probabilístico aleatorio simple, que ha permitido seleccionar a 86 usuarios de la Universidad Nacional Pedro Ruiz Gallo

3.5. Técnicas, Instrumentos, Fuentes e Informantes

A continuación se presentan las técnicas e instrumentos de recolección de información que sirven como ayuda para la realización de este trabajo.

Las técnicas utilizadas para la recolección de información son:

- **Entrevista:** Se realiza una entrevista personal al jefe, para conocer los procesos que tiene el área. También para conocer la problemática respecto a la gestión de seguridad de la información. Para ello se utiliza como instrumento la ficha de entrevista.

- **Análisis documental:** Es el punto de entrada de la investigación, el cual permite conocer sobre el tema. De esta manera se puede rastrear e inventariar los documentos existentes, clasificar los documentos identificados, seleccionar los documentos más importantes, leer en profundidad el contenido.

  Los instrumentos que se utilizaron para recoger y almacenar la información fueron:

- **Formato matricial de análisis, evaluación y tratamiento del SGSI:** Esta técnica permite observar la realidad problemática del servicio de verificación, antes y después de la aplicación del SGSI. El cual mediante la entrevista a los grupos focales se realiza el levantamiento de la información necesaria en cada una de las etapas.

- **Observación de campo:** Esta técnica permite observar la realidad problemática del Área Informática, antes y después de la aplicación de la ISO 27001. Para ello se utiliza como instrumento una ficha de observación.

3.6. Indicadores

Para determinar la contrastación de nuestra investigación entre las operaciones antes del diseño del Sistema de Gestión de la Seguridad de la información y después del mismo, se han determinado los siguientes indicadores:

- ✓ Porcentaje de evaluación de riesgos de seguridad identificados y evaluados con niveles de importancia alta, media o baja
- ✓ Grado de aplicación de políticas de seguridad en la organización
- ✓ Porcentaje de empleados que han recibido y aceptado formalmente, roles y responsabilidades con respecto a seguridad de la información
- ✓ Número de informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización
- ✓ Número y costes acumulados de incidentes por software malicioso como virus, gusanos, troyanos o *spam* detectados y bloqueados
- ✓ Porcentaje de backups y archivos con datos sensibles o valiosos que se encuentran protegidos dentro y fuera de la empresa

- ✓ Número de incidentes de seguridad de red identificados en los meses anteriores, dividido por categorías de leve importante y grave importancia
- ✓ Número de peticiones de cambios de acceso por parte del personal que labora en la empresa
- ✓ Estado de la seguridad en entorno portátil, es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (*laptops*, PDAs, teléfonos móviles, etc.)
- ✓ Porcentaje de sistemas para los cuales los controles de validación de datos se han definido e implementado y demostrado eficaces mediante pruebas
- ✓ Porcentaje de sistemas evaluados de forma independiente conforme a estándares de seguridad básica
- ✓ Numero de informes sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo
- ✓ Número de chequeos (a personas a la salida) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad
- ✓ Porcentaje de nuevos empleados relacionados con las tecnologías de información y comunicaciones (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.

3.7. Desarrollo de Metodología SGSI

Para la implementación de un SGSI se tiene que cumplir con los lineamientos establecidos por la ISO 27001:2005 (clausula 4. Sistema de gestión de seguridad de información) donde describe los

lineamientos y la metodología. A continuación el desarrollo de los siguientes puntos:

- Alcance del Sistema de Gestión de Seguridad de la Información: ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el proceso de alcance y aquellas partes que no hayan sido consideradas.

  A continuación, se adjunta el desarrollo del Alcance documentado, el cual también ha sido firmado por las personas correspondientes de la Oficina Central de Informática (Anexo N° 01).

- Política y objetivos de seguridad: documento de contenido genérico que establece la política de seguridad de información del proceso y el compromiso de la dirección enfocado en la gestión de la seguridad de la información.

  A continuación, se adjunta el desarrollo de la Política y Objetivos de Seguridad de la Información elaborado, el cual también ha sido firmado por las personas correspondientes de la Oficina Central de Informática (Anexo N° 02)

- 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.

ISO 27001 (2005) define el enfoque de evaluación del riesgo de la organización: Identificar una metodología de cálculo del riesgo adecuado para el Sistema de Gestión de Seguridad de la Información y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.

La metodología de estimación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reducibles.

Nota: Existen diferentes metodologías para el cálculo del riesgo.

Es por tales motivos que la metodología desarrollada para el presente proyecto es la Metodología Magerit III siguiendo los lineamientos de la ISO 27001:2005, su análisis de riesgos es una aproximación metódica que permite determinar el riesgo (Anexo 03)

- Análisis y evaluación: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

  A continuación, se adjunta el desarrollo del Informe del Análisis y Evaluación del riesgo, el cual también ha sido firmado por las personas correspondientes de la Oficina Central de Informática (Anexo N° 04)

- Opciones de Tratamiento: Una vez efectuado el análisis y evaluación del riesgo, se debe decidir cómo tratar el riesgo basándonos en las siguientes opciones:

  Reducir: Establecer controles para atenuación (políticas, procedimientos, procesos y herramientas).

Aceptar: Aceptar el riesgo en su presente nivel debido a que no es posible realizar un tratamiento o porque éste resulta demasiado caro.

Transferir: Transferir a un tercero con capacidad financiera / especialización necesaria para administrar el riesgo adecuadamente.

Evitar: Evitar el riesgo eliminándolo de la actividad de la organización.

A continuación, se adjunta el desarrollo del Informe de Opciones de Tratamiento del riesgo, el cual también ha sido firmado por las personas correspondientes de la Oficina Central de Informática (Anexo N° 04).

- Enunciado de aplicabilidad: Documento que contiene los objetivos de control y los controles contemplados por el Sistema de Gestión de Seguridad de la Información, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

  A continuación, se adjunta el desarrollo del Informe del Enunciado de Aplicabilidad de los Riesgos elaborado, el cual también ha sido firmado por las personas correspondientes de la Oficina Central de Informática (Anexo N° 05).

- 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.

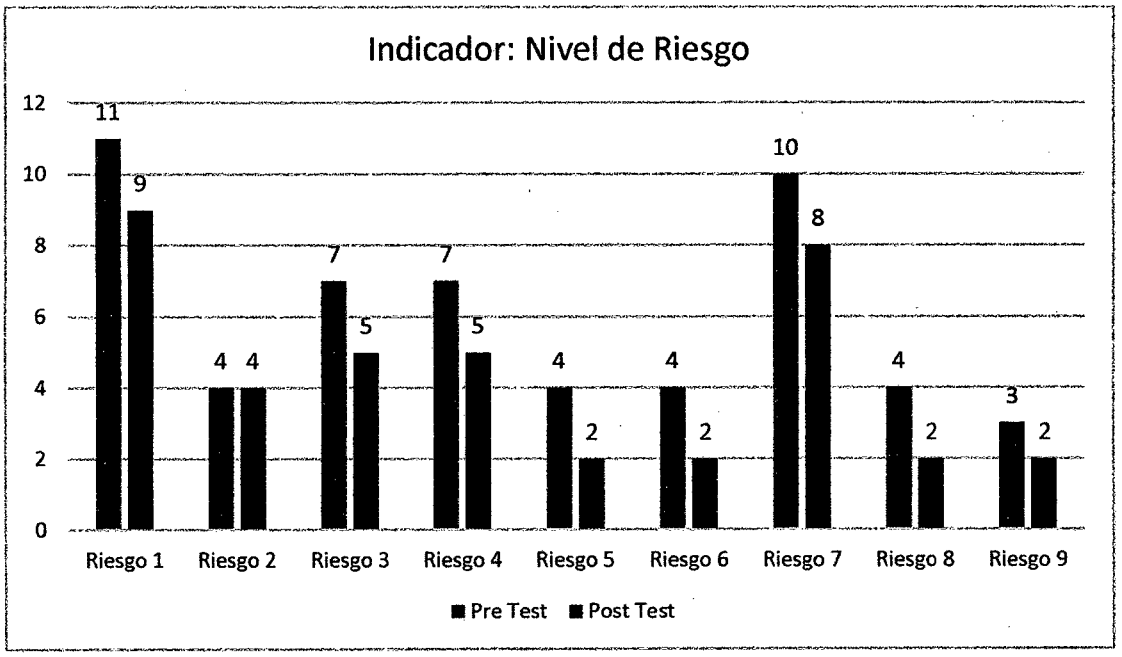
A continuación, se adjunta el desarrollo del Plan de Tratamiento de Riesgos del Proceso, el cual también ha sido firmado por las personas correspondientes de la Oficina Central de Informática (Anexo N° 06).

CAPÍTULO IV
RESULTADOS

"La implementación del Sistema de Gestión de Seguridad de la Información disminuye el nivel de riesgos en el proceso de Soporte de TI de la Oficina Central de Informática."

Gráfico N° 1

Comparación del indicador Nivel de riesgo entre el Pre Test y Post Test

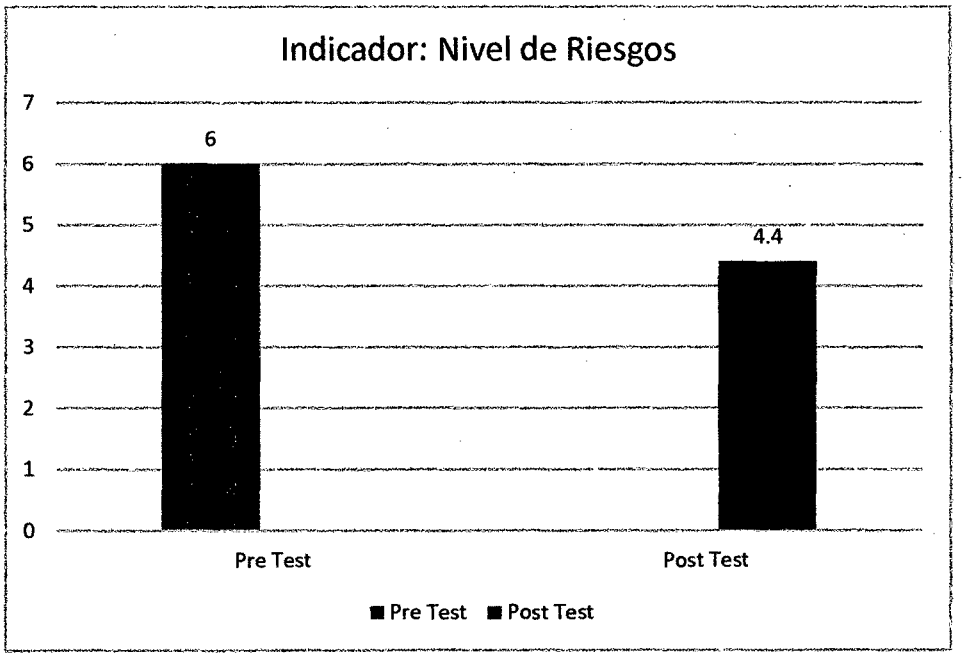


Interpretación:

De acuerdo al gráfico N° 1, se aprecia que el sistema de gestión de seguridad de la Información disminuye el nivel de riesgos de seguridad en el proceso de Soporte e TI de la Oficina Central de Informática, se puede visualizar el pre y post test de los 9 registros de evaluación.

Gráfico N° 2

Variación del Nivel de riesgo – Comparativa General



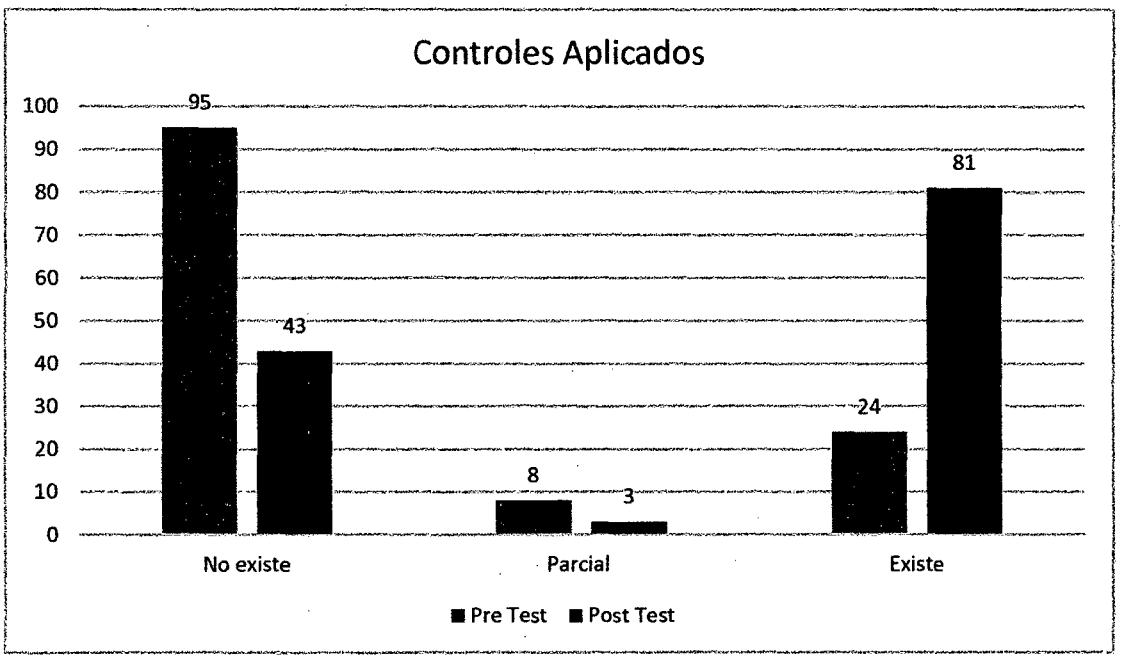
Interpretación:

De acuerdo al gráfico N° 2, se aprecia que existe una disminución de riesgo de 1.6, es decir una disminución del 26.67% utilizando el Sistema de Gestión de Seguridad de la Información en el Proceso de Soporte de TI en la Oficina Central de Informática

"La Implementación del Sistema de Gestión de Seguridad de la Información incrementa los Controles Aplicados en el proceso de Soporte de TI de la Oficina Central de Informática."

Gráfico N° 3

Comparativa general del indicador controles aplicados del Pre Test y Post Test



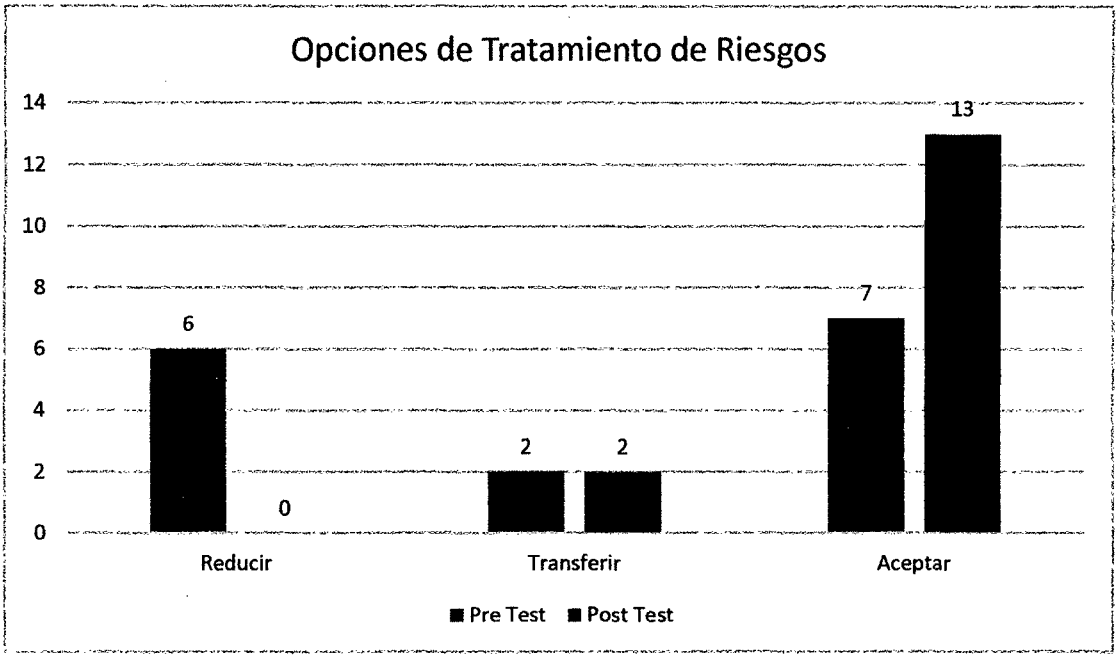
Interpretación:

En el gráfico N° 3 se observa que con la implementación del sistema de gestión de la seguridad de la información se logra disminuir los controles aplicados inexistentes en 40.94% y en consecuencia aumentar los controles aplicados existentes en 44.88 %.

"La Implementación del Sistema de Gestión de Seguridad de la Información mejora las Opciones de Tratamiento de riesgos en el proceso de Soporte de TI de la Oficina Central de Informática."

Gráfico N° 4

Comparativa general del indicador opciones de tratamiento de riesgos aplicados del Pre Test y Post Test



Interpretación:

En el gráfico N° 4 se observa que con la implementación del sistema de gestión de la seguridad de la información se logra disminuir las opciones de tratamiento en "reducir" un 40% y en consecuencia aumentar las opciones de tratamiento en "aceptar" un 46.67%, en este caso es el mismo porcentaje que se agrega en vista de que la las opciones de tratamiento en "transferir", no logra ningún cambio.

CAPÍTULO V
CONCLUSIONES Y SUGERENCIAS

Conclusiones:

- Con el Sistema de Gestión de Seguridad de la Información en el Proceso de Soporte de TI de la Oficina Central de informática - UNPRG, el nivel de riesgo se logra disminuir en promedio de 6 a 4.4, lo que significa un 26.67%. El cual se logra después de haber aplicado la metodología de análisis y evaluación de riesgos, finalizando con la implementación de los controles de la ISO 27001, anexo A., con lo cual se puede afirmar que el nivel de riesgo ha disminuido.

- El riesgo disminuido se le considera riesgo residual, al cual en un nuevo análisis se podrá implementar controles adicionales para su mitigación o control total del riesgo.

- Con la implementación del sistema de gestión de la seguridad de la información se logra disminuir los controles aplicados inexistentes en 40.94% y en consecuencia aumentar los controles aplicados existentes en 44.88 %. La cantidad de controles aplicados inexistentes eran de 95 y con el estándar internacional ISO 27001 se logró reducir a 24. Así mismo, antes de aplicar el estándar internacional ISO 27001 se contaban con 43 controles aplicados existentes, y con su implementación se logró aumentar a 81 controles aplicados, en cuanto a los controles aplicados que se encontraban parcialmente, éstos se redujeron a de 8 a 3. Entonces, los controles aplicados utilizando el estándar internacional ISO 27001 han mejorado.

- La identificación de los riesgos críticos como altos y muy altos son los riesgos que ocasionaran perdidas económicas en las empresas, a los cuales si no se implementa controles de seguridad pueden ocasionar la caída total o parcial de la empresa.

- Con la implementación del sistema de gestión de la seguridad de la información se logra disminuir el riesgo a pérdida económica en un 40%, permitiendo aumentar el riesgo aceptable en un 46.67%, el riesgo aceptable son los considerados con un nivel de criticidad media, baja o muy baja.

Sugerencias:

- Siempre se debe identificar el alcance de cualquier implementación de un SGSI, si no se realiza una buen análisis del ámbito del proceso no se puede realizar una adecuada identificación de los activos de información, el cual es el recurso crítico para la implantación del SGSI

- Profundizar más en la metodología de implementación del Sistema de gestión de seguridad de información con la ISO 27005, donde recientemente se ha documentado y se propone la metodología de implementación.

- Se debe documentar y cumplir no solo con la implementación de los controles del Anexo A de la ISO 27001, esto es un error común de toda implementación del SGSI. Se debe cumplir con lo exigido en la cláusula 4, 5 y 6 del estándar internacional ISO 27001.

- Se puede hacer uso de ITIL como herramienta de apoyo para la implementación de los controles según el correspondiente objetivo de control.

- Se recomienda que en la empresa continúe dando mantenimiento y mejora del Sistema de gestión de seguridad de información, donde se realiza continuamente la revisión de todo el proyecto y la metodología, permitiendo la mejora continua de todo el ciclo PDCA correspondiente a la ISO.

BIBLIOGRAFÍA

Fuentes de Libros impresos

ALEXANDER, A. (Ed.). (2007). *Diseño y Gestión de un Sistema de Seguridad de Información*. Colombia: Alfaomega,

AMPUERO, C. E. (2011). *Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de seguros.* (Tesis para optar Título Profesional), Pontificia Universidad Católica del Perú. <http://tesis.pucp.edu.pe/repositorio/handle/123456789/933 >

AREITIO, J. (2008). *Seguridad de la Información: redes, informática y sistemas de información.* España: Learning Paraninfo S.A.

CALDER, A. (Ed.). (2006). *Information Security based on ISO 27001/ ISO 27002 - A Management Guide.* Alemania: Wilco, Amersfoort-NL.

HERNÁNDEZ, R. (2010). *Metodología de la Investigación Científica.* EE.UU: MC Graw Hill Interamericana.

ISO (2005), Norma técnica Peruana. Adaptado en el año 2008 en el Perú.

LARA, H., REYES, J. y NAVARRETE, W. (2006), *Diseño de sistema de gestión de seguridad de información para Ecuacolor.* (Tesis para optar Título Profesional), Escuela Superior Politécnica del Litoral. <http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-35826.pdf>

MERINO, C. y CAÑIZARES, R. (2011). *Implantación de un sistema de gestión de seguridad de la información según ISO 27001.* España, Barcelona: FC Editorial.

MONTOYA, L. y LOPEZ, M. (2011). *Diseño de una metodología de gestión de riesgos de seguridad de la información para entidades financieras.* (Tesis para optar Título Profesional), Universidad Nacional Mayor de San Marcos.

PALLAS, G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Recuperado el 1 de agosto 2014, de Universidad de la República. Instituto de Computación. <http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf>.

ANEXOS

Anexo 01: Alcance del SGSI

Anexo 02: Política y objetivos de seguridad

Anexo 03: Enfoque de análisis, evaluación y tratamiento de riesgos

Anexo 04: Análisis, evaluación y tratamiento de riesgos

Anexo 05: Enunciado de aplicabilidad

Anexo 06: Plan de tratamiento de riesgos

Oficina Central de Informática - UNPRG	Nro. Documento: **PST-001/01**
	Confidencial

PROCESO DE SOPORTE DE TI

ALCANCE DEL SGSI DEL PROCESO DE SOPORTE DE TI

ÍNDICE

1. INTRODUCCIÓN

El presente documento es uno de los más importantes de la ISO 27001 y la base de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Proceso de Soporte de TI, proceso que se da en la Oficina Central de Informática – UNPRG.
La implementación de los controles del SGSI está regulada por las ISO/IEC 17799:2005 (actualmente ISO 27002:2005) e ISO/IEC 27001:2005. Con la observancia de dichas normas, la Seguridad de la Información estará garantizada en base a la aplicación de procedimientos, normas e instructivos; en lugar de confiar sólo en la implementación de controles tecnológicos en forma aislada.

El alcance y los límites del SGSI se van a definir en función a los aspectos contractuales, las características del negocio (el Core de los procesos) y la ubicación geográfica, con la finalidad de identificar los distintos activos de información que se convierten en el eje principal del modelo del SGSI.

2. OBJETIVOS

Establecer un plan para proteger la información y los activos de la Oficina Central de Informática a través de la confidencialidad, integridad y disponibilidad de los datos.

Definir el ámbito en función a las características del negocio, ubicación geográfica, y red física y lógica del Sistema de Información, donde se va a implementar el Sistema de Gestión de la Seguridad de la Información, en la cual se defina las interfaces de cado uno de los dominios que contienen los activos de información.

3. BASE LEGAL

- NORMA ISO 27001/ 27002 IEC:2005

4. ALCANCE DEL DOCUMENTO

Este documento pretende mostrar una visión general del proyecto a desarrollar, identificando los puntos sobre los cuales se desarrollará la implementación del Sistema de Gestión de la Seguridad de la Información para el Proceso de Soporte de TI de la Oficina Central de Informática de la UNPRG.

5. RESPONSABILIDAD

El jefe de la Oficina Central de Informática es el responsable de revisar y aprobar este documento.

6. DEFINICIONES

- **Acción Correctiva:**

  Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.

- **Activo de información:**
  Es la información o entidad que trata la información y que tiene un valor para la organización.
- **Amenaza:**
  Cualquier acción o evento que puede ocasionar consecuencias adversas.
- **Análisis de Riesgo:**
  Utilización sistemática de la información para identificar las fuentes y estimar el riesgo.
- **Confidencialidad:**
  La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
- **Disponibilidad:**
  La información debe ser disponible en forma organizada para los usuarios autorizados cuando sea requerida.
- **Evento:**
  Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
- **Incidente de seguridad de información:**
  Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazan la seguridad de la información
- **Información:**
  Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
- **Integridad:**
  La información debe ser completa, exacta y válida.
- **Macroproceso:**
  Son los grandes procesos o procesos genéricos de la empresa, que en conjunto dan una visión de cómo opera la organización.
- **Proyecto del SGSI**
  Es un conjunto de actividades planificadas cuyo objetivo es llegar a operar y monitorear el Sistema de Gestión de la Seguridad de la Información, tiene un inicio y un fin.
- **Riesgo:**
  La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos del Proceso de Soporte de TI
- **Seguridad de información:**
  Característica de la información que se logra mediante la adecuada combinación de políticas, estructura organizacional y herramientas informáticas especializadas, a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

- **Tratamiento del riesgo:**
  Proceso de selección e implementación de medidas para modificar el riesgo, para llevarlos a niveles aceptables.
- **Sistema de Gestión de Seguridad de la Información según ISO IEC 27001:**
  Parte del sistema de gestión global, basado en un enfoque de riesgo del negocio, para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Vulnerabilidad:**
  Deficiencias que pueden ser explotadas por amenazas.

7. ABREVIATURAS

- **SGSI:** Sistema de Gestión de Seguridad de Información.
- **ISO:** Organismo Internacional de Estandarización.
- **IEC:** Comisión Electrotécnica Internacional

8. DESCRIPCIÓN

8.1 Situación contractual

Para la implementación del Sistema de Gestión de Seguridad de información para la Oficina Central de Informática, no se cuenta de por medio con un contrato del Proyecto, ya que esto es una investigación de tesis para obtener el Título Profesional.

8.2 Características del negocio

El presente alcance del SGSI está enfocado y delimitado al proceso de Soporte de TI, considerando los siguientes elementos que participan en la actualidad en dicho proceso:

- Hardware Base.
- Software Base y Aplicaciones propios.
- Las comunicaciones propias.
- Los procesos y controles.

8.3 Alcance del Proyecto SGSI

8.3.1 Dominios

Según lo estipulado, se implementarán los siguientes dominios y controles de la Norma ISO/IEC 27002:2005 en el Proceso de Soporte de TI.

Cuadro 1. Alcance del Proyecto SGSI - Dominios ISO/IEC 27001:2005

Dominio 5: POLÍTICAS DE SEGURIDAD

CONTROL	DESCRIPCIÓN
5.1.1	Definir de política de seguridad de la información
5.1.2	Revisión de la política de seguridad de la información

Dominio 6: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE A INFORMACIÓN

CONTROL	DESCRIPCIÓN
6.1.1	Compromiso de la Dirección con la seguridad de la información
6.1.2	Coordinación de la seguridad de la información
6.1.3	Asignación de responsabilidad para la seguridad de la información
6.1.4	Proceso de Autorización de recursos para el tratamiento de la información
6.1.5	Acuerdos de Confidencialidad
6.1.6	Contacto con las autoridades
6.1.7	Contacto con grupos de interés especiales
6.1.8	Revisión independiente de la seguridad de la información
6.2.1	Identificación de riesgos por el acceso de terceros
6.2.2	Tratamiento de la seguridad en la relación con los clientes
6.2.3	Requisitos de seguridad en contratos con terceros

Dominio 7: GESTIÓN DE ACTIVOS

CONTROL	DESCRIPCIÓN
7.1.1	Inventario de activos
7.1.2	Propiedad de los activos
7.1.3	Uso aceptable de los activos
7.2.1	Directrices de clasificación
7.2.2	Etiquetado y manipulado de la información

Dominio 8: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

CONTROL	DESCRIPCIÓN
8.1.1	Funciones y responsabilidades
8.1.2	Investigación de antecedentes
8.1.3	Términos y condiciones de contratación
8.2.1	Responsabilidad de gestión

8.2.2	Concienciación educación y capacitación en seguridad de la información
8.2.3	Proceso disciplinario
8.3.1	Responsabilidad del cese o cambio
8.3.2	Devolución de activos
8.3.3	Retirada de los derechos de acceso

Dominio 9: SEGURIDAD FÍSICA Y AMBIENTAL

CONTROL	DESCRIPCIÓN
9.1.1	Perímetro de seguridad física
9.1.2	Controles físicos de entrada
9.1.3	Seguridad de oficinas, despachos y recursos
9.1.4	Protección contra las amenazas externas y ambientales
9.1.5	El trabajo en áreas seguras
9.1.6	Áreas de acceso público, carga y descarga
9.2.1	Emplazamiento y protección de equipos
9.2.2	Instalaciones de suministro
9.2.3	Seguridad del cableado
9.2.4	Manteniendo de los equipos
9.2.5	Seguridad de los equipos fuera de las instalaciones
9.2.6	Reutilización o eliminación de equipos
9.2.7	Retirada de materiales propiedad de la empresa

Dominio 10: GESTIÓN DE COMUNICACIONES Y OPERACIONES

CONTROL	DESCRIPCIÓN
10.1.1	Documentación de procedimientos de operación
10.1.2	Gestión de cambios
10.1.3	Segregación de tareas
10.1.4	Separación de los recursos de desarrollo , ensayo y producción
10.2.1	Prestación de servicios
10.2.2	Supervisión y revisión de los servicios prestados por terceros
10.2.3	Gestión de cambios en los servicios prestados por terceros
10.3.1	Gestión de capacidades
10.3.2	Aceptación del sistema
10.4.1	Controles contra el código malicioso
10.4.2	Controles contra el código descargado en el cliente
10.5.1	Copias de seguridad de la información
10.6.1	Controles de red
10.6.2	Seguridad de los servicios de red
10.7.1	Gestión de soporte extraíble
10.7.2	Eliminación de soportes

10.7.3	Procedimientos de manejo de la información
10.7.4	Seguridad de la documentación del sistema
10.8.1	Políticas y procedimientos de intercambio de información
10.8.2	Acuerdo de intercambio
10.8.3	Soportes físicos en tránsito
10.8.4	Mensajería electrónica
10.8.5	Sistema de Información de empresa
10.9.1	Comercio electrónico
10.9.2	Transacciones el línea
10.9.3	Información a disposiciones pública
10.10.1	Registro de auditorías
10.10.2	Supervisión de uso del sistema
10.10.3	Protección de la información de registro
10.10.4	Registro de administración y operación
10.10.5	Registro de fallos
10.10.6	Sincronización de relojes

Dominio 11: CONTROL DE ACCESOS

CONTROL	DESCRIPCIÓN
11.1.1	Políticas de control de accesos
11.2.1	Registro de usuario
11.2.2	Gestión de privilegios
11.2.3	Gestión de contraseñas de usuario
11.2.4	Revisión de los derechos de acceso de los usuarios
11.3.1	Uso de contraseña
11.3.2	Equipo informático de usuario desatendido
11.3.3	Política de puesto de trabajo despejado y bloqueo de pantalla
11.4.1	Políticas de uso de los servicios de red
11.4.2	Autentificación de usuarios para conexiones externas
11.4.3	Identificación de equipos de redes
11.4.4	Diagnóstico remoto y protección de los puertos de configuración
11.4.5	Segregación en redes
11.4.6	Control de la conexión a red
11.4.7	Control de encaminamiento de red
11.5.1	Procedimientos seguros de inicio de sesión
11.5.2	Identificación y autentificación de usuario
11.5.3	Sistema de gestión de contraseñes
11.5.4	Uso de las utilidades de sistema
11.5.5	Desconexión automática de sesiones
11.5.6	Limitación del tiempo de conexión
11.6.1	Restricción de accesos a la información

11.6.2	Aislamiento de sistemas sensibles

Dominio 12: ADQUISICIÓN ,DESARROLLO Y MANTENIMIENTO

CONTROL	DESCRIPCIÓN
12.1.1	Análisis y especificación de los requisitos de seguridad
12.2.1	Validación de los datos iniciales
12.2.2	Control del procesamiento interno
12.2.3	Autenticación e integridad de los mensajes
12.2.4	Validación de los datos de salida
12.3.1	Política de uso de los controles criptográficos
12.3.2	Gestión de claves
12.4.1	Control del software en explotación
12.4.2	Protección de los datos de pruebas del sistema
12.4.3	Control de acceso al código fuente de los programas
12.5.1	Procedimientos de control de cambios
12.5.2	Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo
12.5.3	Restricciones a los cambios en los paquetes de software
12.5.4	Fuga de información
12.5.5	Externalización del desarrollo de software
12.6.1	Control de las vulnerabilidades técnicas

Dominio 13: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

CONTROL	DESCRIPCIÓN
13.1.1	Notificación de los eventos de seguridad de la información
13.1.2	Notificación de puntos débiles de la seguridad de la información
13.2.1	Responsabilidades y procedimientos
13.2.2	Aprendizaje de los incidentes de seguridad de la información
13.2.3	Recopilación de evidencias

Dominio 14: GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

CONTROL	DESCRIPCIÓN
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
14.1.2	Continuidad del negocio y evaluación de riesgos
14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información
14.1.4	Marco de referencia para la planificación del contenido de negocio
14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad

Dominio 15: CUMPLIMIENTO

CONTROL	DESCRIPCIÓN
15.1.1	Identificación de la legislación aplicable
15.1.2	Derechos de propiedad intelectual(DPI)
15.1.3	Protección de los registros de la organización
15.1.4	Protección de datos y privacidad de la información personal
15.1.5	Prevención del uso indebido de las instalaciones de procesamiento de la información
15.1.6	Regulación de los controles criptográficos
15.2.1	Cumplimiento de las políticas y normas de seguridad
15.2.2	Comprobación del cumplimiento técnico
15.3.1	Controles de auditoría de los sistemas de información
15.3.2	Protección de la herramientas de auditoría de los sistemas de información

Si en el transcurso del Proyecto SGSI se juzga como necesaria y conveniente la implementación de controles adicionales, dentro de los dominios mencionados en el Cuadro 1, estos serán incluidos en el documento "Plan de Tratamiento del Riesgo".

8.4 Ubicación Geográfica

El sistema cubrirá los procesos y activos de información de la Universidad Nacional Pedro Ruiz Gallo para el proceso de Soporte de TI:

- Universidad Nacional Pedro Ruiz Gallo - Av. Juan XXIII, N° 339, Lambayeque.

Oficina Central de Informática - UNPRG	Nro. Documento: **PST-002/01** CONFIDENCIAL

PROCESO DE SOPORTE DE TI

OBJETIVOS Y POLITICAS DEL SGSI PARA EL PROCESO DE SOPORTE DE TI|

ÍNDICE

1. OBJETIVO DEL DOCUMENTO

El Documento de Políticas y Objetivos de Seguridad de la Información persigue los siguientes fines:

- Dar soporte al Sistema de Gestión de la Seguridad de la información (SGSI) de la organización. Las políticas son los principios o conceptos que sirven como base para los objetivos del sistema y el diseño los de Procedimientos de Seguridad de la Información, o la mejora de los existentes.
- Establecer las bases para una cultura de seguridad de la información en todos los miembros del Proceso de Soporte de TI. Esta tarea será complementada con la implementación de Procedimientos de seguridad y con la Concientización y Capacitación en temas de seguridad de la información.
- Asegurar que los objetivos del SGSI sean adecuados a las necesidades y requerimientos de la organización.

2. BASE LEGAL

- NORMA ISO 27001/ 27002 IEC:2005, capítulo 4.2.1

3. ALCANCE

Estas políticas deben ser conocidas y cumplidas por todos los empleados del Proceso de Soporte de TI, sin excepción alguna, sea cual fuere su nivel jerárquico, y bajo cualquier modalidad.

4. RESPONSABLE

El director de la Oficina Central de Informática – UNPRG es el responsable de revisar y aprobar este documento.

5. POLÍTICA DEL SGSI DEL PROCESO DE SOPORTE DE TI

Somos una unidad responsable de planificar y mantener operativa la plataforma tecnológica de hardware y software instalada en las áreas usuarias d las diferentes unidades académicas y administrativas de la universidad. La seguridad tanto de la información como de los sistemas que soportan dicha información es de vital importancia para la organización.

La información en cualquier medio debe ser almacenada y tratada bajo los niveles de seguridad adecuados al estado actual de la tecnología. Estos niveles de seguridad se basarán en los controles y objetivos establecidos en la **normativa ISO/IEC 27001.**

El Jefe del Proceso de Soporte de TI de la Oficina Central de Informática apoya y ha aprobado la presente Política del SGSI. Es responsabilidad de todos los empleados del Proceso de Soporte de TI adherirse y cumplir la Política de Seguridad de la Información, sin excepción alguna, sea cual fuere su nivel jerárquico, y bajo cualquier modalidad.

Para lograr lo anterior nos comprometemos a:

- Conocer y cumplir con la política general de Seguridad de la Información y toda otra política, reglamento o procedimiento que el Proceso de Soporte de TI considere necesario implantar para cumplir con los requisitos legales y/o salvaguardar la integridad, disponibilidad y confidencialidad de la información vigentes en la Oficina Central de Informática.

- Asumir la responsabilidad sobre los sistemas y recursos puestos a mi disposición para el desarrollo de las funciones que se me encomendó. Me responsabilizo por la seguridad de los mismos.
- Notificar al a mi jefe inmediato, en caso de verificar el mal uso de los recursos por parte de algún otro empleado interno o externo del Proceso de Soporte de TI.
- Utilizar sólo aquel software que esté autorizado por el área competente y que me haya sido asignado para el desarrollo de las funciones encomendadas.
- Asumir la responsabilidad en el uso y manipulación de la información sobre la que tengo autorización, la que me comprometo a efectuar y proteger en base a los niveles de clasificación que tenga dicha información.
- Me comprometo a no acceder, copiar ni transferir información para la cual no tengo la autorización adecuada.
- Participar de la capacitación y evaluación periódica del personal en temas referentes a la seguridad de la información.
- Gestionar eficiente y eficazmente las incidencias de la seguridad de información.

Ing. Luis Delfín	**Ing. Luis Alberto Reyes Lescano**
Jefe de Soporte de TI	**Director de la Oficina Central de Informática**

6. OBJETIVOS DEL SGSI

El Jefe de Unidad de Sistemas ha definido los siguientes objetivos del SGSI:

1. Contribuir con el aseguramiento de la confidencialidad, integridad y disponibilidad de la información y de los equipos que procesan la información utilizada por Proceso de Soporte de TI para sus procesos de importantes.
2. Incrementar el conocimiento y la conciencia del personal del Proceso de Soporte de TI en las buenas prácticas de seguridad de la información.
3. Preparar al Proceso de Soporte de TI para una certificación de la ISO/IEC 27001:2005.

La ejecución y evaluación del cumplimiento de la Política y Objetivos del SGSI deberán ser revisadas y actualizadas anualmente, según sea necesario.

Ing. Luis Delfín	**Ing. Luis Alberto Reyes Lescano**
Jefe de Soporte de TI	**Director de la Oficina Central de Informática**

Oficina Central de Informática - UNPRG	Nro. Documento: **PST-003/01**
	CONFIDENCIAL

PROCESO DE SOPORTE DE TI

INFORME DEL ANÁLISIS Y EVALUACIÓN DEL RIESGO

ÍNDICE

1. OBJETIVO

Desarrollar el análisis y evaluación de riesgos del proceso de Soporte de TI según alcance, como resultado de la valorización de los activos, identificación de las amenazas. Vulnerabilidades y controles existentes.

2. BASE LEGAL

ISO/IEC 27001:2007 Sistema de Gestión de la Seguridad de la Información (SGSI)- Requisitos, 4.2.1 Establecimiento del SGSI, numerales d),e),f).

3. ALCANCE

Este documento es elaborado para realizar el análisis y evaluación del Riesgo del proceso de Soporte de TI según el documento del Alcance del SGSI.

4. DEFINICIONES

4.1 Información: Datos que poseen significado.

4.2 Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

4.3 Integridad: Garantía de la exactitud y el contenido completo de la información. Asegurar de Proteger a la información de cualquier modificación o destrucción no autorizada.

4.4 Disponibilidad: Asegurar el acceso a la información por parte de los usuarios autorizados en el momento que ellos lo requieran.

4.5 Activo de Información: La información y su medio de soporte (por ejemplo, expediente, bases de datos) así como los activos asociados con el procesamiento de información (computadoras, red interne, aplicativos).

4.6 Propietario del activo: El término propietario identifica a un individuo o entidad que tiene responsabilidad de gestión aprobada para controlar la producción, desarrollo, mantenimiento, utilización y seguridad de los activos. El término "propietario" no significa que la persona actualmente tiene derechos de propiedad sobre el activo.

4.7 Custodia del activo: Es el usuario dispuesto por el propietario del activo responsable de resguardad los activos de información que utiliza y/o custodia.

4.8 Clasificación de la Información

Es aquel proceso por el que se caracteriza a los diferentes tipos de información.
En el Proceso de Soporte de TI ha sido clasificada de la siguiente manera:

CLASIFICACIÓN	DESCRIPCIÓN
Información Confidencial	Información a la cual solo tienen acceso un número reducido de usuario. Si se produce un acceso no autorizado puede impactar significantemente contra la organización, clientes, personal o terceros.
Información Restringida	Información utilizada por el personal para conducir las operaciones del negocio, y que puede ser compartido con terceros en forma autorizada.
Información Pública	Información disponible para distribuir al público, siguiendo procedimientos o canales establecidos. Información de dominio público.

4.9 Tipos de Activo

Puede resultar conveniente dividir los activos de información según su estado y características propias. A modo de ejemplo, se muestran los siguientes tipos:

- **Recurso de Información**: Información que se encuentra impresa o manuscrita, tangible o intangible que se utiliza para ciertas actividades del proceso.
- **Software**: Conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina.
- **Hardware**: Corresponde al equipamiento informático (Pcs, laptops, servidores), equipos de comunicaciones y seguridad (routers, hubs, switches, redes, firewalls, IDPs, Secure Access, entre otros), medios magnéticos (cintas, CDs, y discos).
- **Servicios**: Tales como Energía Eléctrica, Agua, Red, Conexión VPN, telefonía, ente otros Estos servicios se apoyan generalmente en elementos de hardware (cables, tubos, etc.) pero los usuarios los perciben como servicios.
- **Personal**: Incluye a todo el personal involucrado en el proceso, en este caso del proceso de Soporte de TI.

4.10 Amenaza

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Algunos ejemplos de Amenaza: Adulteración de documentos, Fuga de información, Incendio, Terremoto, Código Malicioso, Caída Eléctrica, Falla en los Servicios de Comunicación, etc.

4.11 Vulnerabilidad

Es la debilidad de un activo o grupo de activos, que pueden ser explotadas por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.
Algunos ejemplos de vulnerabilidad: que no se cuente con personal capacitado, falta de control de privilegios del sistema, errores de programación, etc.

4.12 Control

Significa el manejo del riesgo, lo que puede incluir políticas, procedimientos, guías, prácticas, nuevo equipos o nuevas estructuras organizaciones; las cuales pueden tener naturaleza administrativa, técnica, legal o de gestión. El término Control es también utilizado como sinónimo de salvaguarda o contramedida. Los controles pueden ser preventivos, detectores, correctivos o persuasivos.

- **Los controles preventivos** sirven para que la amenaza no cumpla con su objetivo de atentar contra la seguridad del activo, por ejemplo, la delimitación del perímetro de la seguridad física.
- **Los controles detectores** son aquello que sirven para descubrir amenazas o vulnerabilidades de la seguridad de la información, por ejemplo instalar un software detector de intrusos (IDS).
- **Los controles disuasivos** sirven para que el agente de la amenaza desiste de tomar acciones que atenta contra la seguridad de la información de los activos. Un ejemplo son los procesos disciplinarios.
- **Los controles correctivos** son aquellos que se ejecutan después de un ataque contra la seguridad de la información y sirven para corregir el daño en la seguridad que ha sufrido el activo. Un ejemplo es la inclusión de cámaras de seguridad después de sufrir un robo en la organización.

4.13 Controles Existentes

Son aquellos controles que ya se encuentran implementados por la organización, previamente el análisis de Riesgo realizado.

4.14 Degradación

Es el grado en que se ve afectado al activo de información, cuando una vulnerabilidad es explotada por una amenaza, tomando en cuenta los controles existentes.

4.15 Impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, se deriva el impacto que estas tendrían.

4.16 Probabilidad

Posibilidad de que se materialice la amenaza, es decir, que se produzca un ataque éxitos, tomando en cuenta las vulnerabilidades y los controles existentes.

4.17 Riesgo

Se denomina riesgo a la medida del daño probable sobre un activo. Conociendo el impacto de las amenaza sobre los activos, se deriva el riesgo sin más que tener en cuenta la probabilidad de ocurrencia de la amenaza.

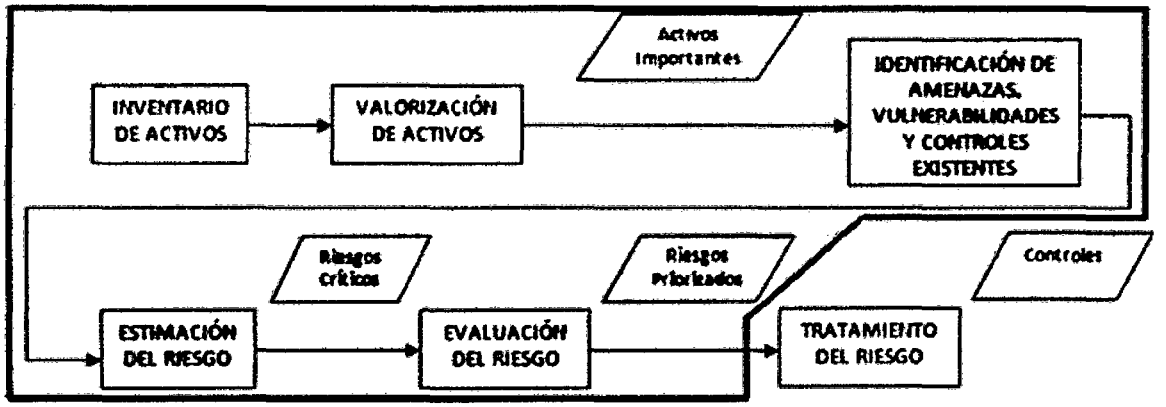
5. ABREVIATURAS

5.1 SGSI: Sistemas de Gestión de Seguridad de la Información

6. METODOLOGÍA DEL ANÁLISIS, EVALUACIÓN Y OPCIONES DE TRATAMIENTO DEL RIESGO

La metodología de Gestión del Riesgo se ha dividido en 4 partes:

i. Inventario de Activos de Información.
ii. Análisis del Riesgo.
iii. Evaluación del Riesgo.
iv. Opciones de Tratamiento del Riesgo.



7. INVENTARIO Y VALORIZACIÓN DE ACTIVOS DE INFORMACIÓN

El inventario y la valorización se adjunta en el **Anexo 01**, a continuación se resume el proceso de identificación y valorización de activos de acuerdo a la metodología.

7.1. Inventario de Activos:

Los activos relevantes han sido identificados y posteriormente tasados por un grupo multidisciplinario compuesto por personas (los propietarios) involucrados en el proceso y subprocesos que abarca el alcance del SGSI.

Por cada activo de definió:

- Código
- Nombre
- Clasificación (si la tuviera)
- Tipo
- Propietario
- Proceso al que pertenece

7.2. *Valorización de Activos*

La valorización de los activos de información se realizó para cada proceso en cuanto a su Confidencialidad, Integridad y Disponibilidad (CID). Los valores de importancia están en una escala penta:

Escala	Valor de Importancia
1	MUY BAJO
2	BAJO
3	MEDIO
4	ALTO
5	MUY ALTO

Tabla N°1

El Valor General del Activo resulto del promedio de los valores CID promediados en cada proceso.

7.2.1. Criterios para la Valorización de los Activos

Los criterios utilizados para valorar los activos de información fueron los siguientes:

✓ **En cuanto a su Confidencialidad**

5: MA
El uso y/o divulgación no autorizada tiene como consecuencia grave perjuicio económico.
El uso y/o divulgación no autorizada conlleva a problemas legales graves y fuertes sanciones.
El uso y/o divulgación no autorizada afecta seriamente la imagen de la organización.

4: A
El uso y/o divulgación no autoriza tiene como consecuencia perjuicio económico moderado.
El uso y/o divulgación no autorizada conlleva a problemas legales moderados y leves sanciones.
El uso y/o divulgación no autorizada puede afectar la imagen de la organización.
3: M
El uso y/o divulgación no autoriza tiene perjuicio económico no significativo.

El uso y/o divulgación no autorizada conlleva a problemas administrativos y operativos internos.
El uso y/o divulgación no autorizada no afecta la imagen de la organización.

2: B
El uso y/o divulgación no autoriza no tiene perjuicio económico.
El uso y/o divulgación no autorizada conlleva a problemas administrativos y operativos internos no significativos.
El uso y/o divulgación no autorizada no afecta la imagen de la organización.

1: MB
El uso y/o divulgación dentro de la organización no requiere autorización.
El uso y/o divulgación no conlleva a problemas legales, ni sanciones.
El uso y/o divulgación no conlleva a problemas administrativos ni operativos internos.
El uso y/o divulgación no afecta la imagen de la organización.

✓ **En cuanto a su Integridad**
5: MA
La modificación y/o eliminación del activo de la información sin autorización compromete gravemente los procesos y operaciones de la organización.
La modificación, eliminación y/o réplica del activo de la información sin autorización puede conllevar a graves problemas legales y fuertes sanciones.

4: A
La modificación y/o eliminación del activo de la información sin autorización compromete moderadamente los procesos y operaciones de la organización.
La modificación, eliminación y/o réplica del activo de la información sin autorización puede conllevar a problemas legales moderados y a leves sanciones.

3: M
La modificación y/o eliminación del activo de la información sin autorización no afecta significativamente a los procesos y operaciones de la organización.
La modificación, eliminación y/o réplica del activo de información sin autorización puede conllevar a problemas administrativos.

2: B
La modificación y/o eliminación del activo de la información sin autorización no afecta a los procesos y operaciones de la organización.
La modificación, eliminación y/o réplica del activo de información sin autorización no conlleva a problemas administrativos.

1: MB
La modificación y/o eliminación del activo de la información no requiere autorización.

✓ **En cuanto a su disponibilidad**
5: MA
La modificación de información es indispensable para los procesos críticos de la organización.
Imposibilita el cumplimiento de la misión y funciones de la organización.

4: A
El activo de información es indispensable para los procesos operativos de la organización.
Demoras considerables en la entrega del servicio o producto.

3: M
El activo de información se considera de soporte a los procesos operativos de la organización.
Demoras tolerables en la entrega del servicio o producto.

2: B
El activo de información se considera de soporte secundario a los procesos operativos de la organización.
No genera demoras en la entrega del servicio o producto.

1: MB
No indispensable para los procesos de la organización.

8. ANÁLISIS DE RIESGO

El análisis del riesgo se adjunta en el **Anexo02**, a continuación se resume el proceso del análisis según la metodología:

8.1. Amenazas, vulnerabilidades y Controles Existentes

En el análisis de riesgos se identificaron **amenazas y vulnerabilidades** a las cuales están expuestos los activos de información relevantes que pasaron a esta etapa, así como los **controles existentes** que se tiene para proteger a los activos.

Las amenazas fueron clasificadas de la siguiente manera:

- Error y Fallo no intencionados.
- Ataques intencionados.
- Influencia Social o económico.
- Desastres naturales
- Origen industrial

Las vulnerabilidades fueron Clasificadas de la siguiente manera:

- Seguridad de los Recursos Humanos.
- Control de Accesos.
- Seguridad Física y Ambiental.
- Gestión de Operaciones y Comunicaciones.
- Mantenimiento, Desarrollo y Adquisición de Sistemas.

8.2. Degradación del Activo

Considerando las vulnerabilidades y controles existentes para cada activo en cuanto a las dimensiones de Confidencialidad, Integridad y Disponibilidad (CID), se obtiene el valor de ***Degradación*** de los activos con las amenazas. Los valores de degradación están en una escala penta:

Escala	Valor de Importancia
1	MUY BAJO
2	BAJO
3	MEDIO
4	ALTO
5	MUY ALTO

Tabla N° 4

La degradación final es la ***Degradación Máxima*** estimada en el CID por cada activo y amenaza.

8.2.1. Criterios para Estimar la Degradación de los Activos

Los criterios para estimar la degradación de los activos de información fueron los siguientes:

En cuanto a su confidencialidad
5: MA
El activo de información es expuesto y es imposible impedir su divulgación y/o copia y no se puede tomar medidas de remediación

4: A
El activo de información es expuesto y es posible detener su divulgación y/o copia.

3: M
El activo de información es expuesto y se puede tomar medidas de remediación.

2: B
El activo de información es expuesto y no re requiere tomar medidas de remediación.

1: MB
La exposición no afecta al activo de información.

En cuanto a su integridad
5: MA
Imposible de recuperar el documento al 100%.

4: A
Se puede reconstruir con suma dificultad.

3: M
Se puede reconstruir con media dificultad.

2: B
Se puede obtener copias, aunque su obtención no es inmediata.

1: MB
Resulta fácil obtener la copia del activo.

En cuanto a su disponibilidad
5: MA
No disponible nunca más.

4: A
Disponible en más de una semana.

3: M
Disponible en 3-5 días útiles.

2: B
Disponible en 1-2 días útiles.

1: MB
Disponible en cuestión de horas.

8.3. Determinación del Valor de Impacto

El impacto toma en cuenta la Degradación, así como el Valor del Activo. La fórmula es la siguiente:

$$\text{IMPACTO} = (\text{Degradación}_{(\text{máx.})} + \text{Valor Activo}) / 2$$

Los valores del Impacto se redondean al valor entero más próximo, como se muestran en la siguiente escala:

Promedio Aritmético	Valor del Impacto	Significado
[1 - 1.4]	1 (MB)	MUY BAJO
[1.5 - 2.4]	2 (B)	BAJO
[2.5 - 3.4]	3 (M)	MEDIO
[3.5 - 4.4]	4 (A)	ALTO
[4.5 - 5]	5 (MA)	MUY ALTO

8.4. Determinación de la Probabilidad

La probabilidad es la posibilidad de que se materialice una amenaza, es decir, que se produzca un ataque exitoso de una amenaza, tomando en cuenta las vulnerabilidades y los controles existentes. Para el presente análisis se toman en cuenta los siguientes valores de probabilidad en una escala penta:

Escala	Valor de Importancia
1	MUY BAJO
2	BAJO
3	MEDIO
4	ALTO
5	MUY ALTO

8.4.1. Criterios para estimar la Probabilidad de Ocurrencia de una Amenaza

Ocurrencia (frecuencia) de que la amenaza afecte al activo de Información
5: MA
Se puede presentar a diario o casi a diario.

4: A
Se puede presentar mensualmente.

3: M
Se puede presentar al menos una vez al año.

2: B
Se puede presentar una vez entre 1 a 3 años.

1: MB
Se puede presentar cada varios años.

8.5. Estimación del Riesgo

El riesgo es la combinación de la probabilidad de una amenaza se materialice y las consecuencias que acarrea dicho ataque (Impacto). La fórmula es la siguiente:

RIESGO = (Impacto + Probabilidad)/2

Los valores del Impacto se redondean al valor entero más próximo, como se muestra en la siguiente tabla:

MATRIZ RIESGO			IMPACTO				
			Muy Bajo	Bajo	Medio	Alto	Muy Alto
			1	2	3	4	5
PROBABILIDAD	Muy Bajo	1		2	2	3	3
	Bajo	2	2	2	3	3	4
	Medio	3	2	3	3	4	4
	Alto	4	3	3	4	4	5
	Muy Alto	5	3	4	4	5	5

8.5.1. Criterio de Aceptación del Riesgo

El criterio de aceptación del riesgo se detalla en la siguiente tabla:

ESCALA	VALOR DEL RIESGO	SIGNIFICADO
	RIESGO MUY BAJO	Es un riesgo aceptable cuando el activo se encuentra expuesto a riesgos leves o moderados, por lo que NO amerita que sean tratados.
2	RIESGO BAJO	
3	RIESGO MEDIO	
4	RIESGO ALTO	El activo se encuentra expuesto a riesgos altos o críticos y necesita ser tratado.
5	RIESGO MUY ALTO	

Los Riesgos Altos (4) y Muy Altos (5) pasarán a la fase de Evaluación del Riesgo.

9. EVALUACIÓN DEL RIESGO

Luego de efectuado el cálculo del valor del riesgo, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos desde el punto de vista de la organización, para poder jerarquizarlos por su importancia.

A continuación se muestran los Criterios para la Evaluación del Riesgo que van a ser utilizados por la organización para evaluar la importancia del riesgo:

Criterios	Descripción
ECONÓMICO	Cuando el impacto económico de la amenaza es mayor a un porcentaje del costo mensual del servicio, o a un número determinado de U.I.T.
CONTINUIDAD	Cuando se paraliza un proceso de línea o al menos una actividad importante del mismo.
LEGAL	Aplica cuando el impacto ocasiona una demanda de índole civil o una denuncia de índole penal al proveedor, lo cual ocasionaría la aplicación de una sanción y/o una indemnización en la vía civil o reparación en la vía penal.
IMAGEN	Cuando la amenaza puede ocasionar que se vea afectada la imagen de la institución y/o proveedores ante terceros (pensionistas, solicitantes, público en general).
CONTRACTUAL	Cuando el impacto amenaza el cumplimiento de contrato, debido a causas previsibles o no, siempre que se hallen determinados en el contrato.

ANEXOS

ANEXO 01
INVENTARIO Y VALORIZACIÓN DE ACTIVOS

INVENTARIO

N°	Cod	Nombre del Activo	Tipo	Descripción del Activo	Ubicación	Gerencia / Área / Servicio asignado	Propietario / Custodio
1	ST.HW.001	Switch	Hardware	Es el dispositivo de comunicación entre todas las áreas.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
2	ST.HW.002	Patch Panel	Hardware	Es un organizador de conexiones de red.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
3	ST.HW.003	PCs	Hardware	Son las computadoras personales mediante se envía correos indicando las incidencias a solucionar al auxiliar de soporte.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
4	ST.HW.004	Impresora	Hardware	Es un dispositivo en la cual le permite imprimir los Registros de Incidencias y demás.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
5	ST.HW.005	Teléfono Ip	Hardware	Medio por el cual informan las incidencias de las distintas áreas	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
6	ST.HW.006	Soplete	Hardware	Dispositivo el cual sirve para dar mantenimiento preventivo a equipo informáticos	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
7	ST.HW.007	Lectora externa DVD	Hardware	Dispositivo donde se almacenan programas necesarios para el buen funcionamiento de los equipos informáticos.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín

N°	Cod	Nombre del Activo	Tipo	Descripción del Activo	Ubicación	Gerencia / Área / Servicio asignado	Propietario / Custodio
8	ST.HW.010	Estabilizador	Hardware	Es un dispositivo eléctrico que permite controlar la transmisión eléctrica hacia los equipos informáticos.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
9	ST.INF.001	Registro de Incidencias	Información	Documento donde se lleva el control de todas las incidencias que fueron atendidas.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
10	ST.INF.002	Orden de salida de equipos	Información	Documento con el cual se permite la salida de equipos informáticos fuera del campus universitario	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
11	ST.INF.003	Formato de préstamo de equipo	Información	Está orientado a los usuarios quienes necesitan cambio de equipo informático	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
12	ST.INF.004	CD/DVD/HDD Externo	Información	Dispositivos los cuales permiten dar soluciones informáticas a los incidentes informados.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
13	ST.PER.001	Jefe de Unidad de Soporte	Personal	Es el encargado del buen funcionamiento de dispositivos periféricos dentro de la organización.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
14	ST.PER.002	Encargada de Help Desk	Personal	Se encarga de registrar e informar la incidencia reportada al personal a cargo.	Oficina Central de Informática	Unidad de Soporte de TI	Pamela Colunche
15	ST.PER.003	Auxiliares de Soporte de TI	Personal	Encargado de atender las incidencias reportadas.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín

N°	Cod	Nombre del Activo	Tipo	Descripción del Activo	Ubicación	Gerencia / Área / Servicio asignado	Propietario / Custodio
16	ST.SW.001	Antivirus Corporativo NOD32	Software	Es el encargado de la seguridad de la información sobre posibles ataques informáticos (virus)	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
17	ST.SW.002	Correo electrónico institucional	Software	Se encarga de enviar mensajes entre distintos usuarios internos y externos para atender sus necesidades informáticas.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
18	ST.SW.003	Microsoft Excel	Software	Una hoja de cálculo donde se almacena información referente a todos los registro de incidencias y atenciones.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
19	ST.SER.001	Servicio Eléctrico	Servicios	Es el conductor de electricidad que es primordial dentro de la organización para su buen funcionamiento de ella.	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín
20	ST.SER.002	Internet	Servicios	Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, en la cual se emplea para poder tener actualizado los distintos software y dar solución a los distintos problemas informaticos que se presentan	Oficina Central de Informática	Unidad de Soporte de TI	Luis Delfín

TASACIÓN

	ACTIVO DE INFORMACION				TASACION DEL ACTIVO				
N°	Cod	Activo	Clasificación	Propietario/Responsable	Confidencialidad	Integridad	Disponibilidad	Valor de tasación	Nivel de tasación
1	ST.HW.001	Switch	Restringido	Luis Delfín	4	4	5	4	Alto
2	ST.HW.002	Patch Panel	Restringido	Luis Delfín	3	4	4	4	Alto
3	ST.HW.003	PCs	Restringido	Luis Delfín	3	3	4	3	Medio
4	ST.HW.004	Impresora	Restringido	Luis Delfín	3	3	3	3	Medio
5	ST.HW.005	Teléfono Ip	Restringido	Luis Delfín	3	3	4	3	Medio
6	ST.INF.001	Registro de Incidencias	Confidencial	Luis Delfín	3	4	3	3	Medio
7	ST.INF.002	Orden de salida de equipos	Restringido	Luis Delfín	4	4	3	4	Alto
8	ST.INF.003	Formato de préstamo de equipo	Restringido	Luis Delfín	4	4	3	4	Alto
9	ST.INF.004	Cd/DVD/Disco Duro Externo	Restringido	Luis Delfín	3	3	3	3	Medio
10	ST.PER.001	Jefe de Unidad de Soporte	Confidencial	Luis Delfín	5	4	5	5	Muy alto
11	ST.PER.002	Encargada de Help Desk	Confidencial	Luis Delfín	5	4	5	5	Muy alto
12	ST.PER.003	Auxiliar de Soporte	Restringido	Luis Delfín	4	3	3	3	Medio
13	ST.SW.001	Antivirus Corporativo NOD32	Restringido	Luis Delfín	3	4	5	4	Alto
14	ST.SW.002	Correo electrónico	Restringido	Luis Delfín	4	3	3	3	Medio
15	ST.SW.003	Microsoft Excel	Restringido	Luis Delfín	4	3	4	4	Alto
16	ST.SER.001	Servicio Eléctrico		Luis Delfín	4	5	4	4	Alto
17	ST.SER.002	Internet		Luis Delfín	3	3	3	3	Medio
18	ST.SER.004	Soplete		Luis Delfín	3	3	3	3	Medio
19	ST.SER.005	Lectora Externa DVD		Luis Delfín	3	3	3	3	Medio
20	ST.SER.006	Estabilizador		Luis Delfín	3	3	3	3	Medio

ANEXO 02
ANÁLISIS DEL RIESGO DEL PROCESO

Activo Crítico				Amenazas Potenciales		Vulnerabilidad Importantes		Analisis del Riesgo							
N°	Código del Activo	Activo	Valor del Activo	Código Amenaza	Amenaza	Código Vulnerabilidad	Vulnerabilidad	Controles existentes	Degradación			Degradación Máxima	Impacto	Probabilidad	Riesgo
									C	I	D				
1	BD.HW.001	Switch	4	AAI22	Manipulación de la configuración	VRH07	Falta de procesos disciplinarios formales		3	3	3	3	4	3	4
	BD.HW.001		4	AEF12	Errores de mantenimiento / actualización de equipos (hardware)	VRH02	Empleados desmotivados		3	-	3	3	4	2	3
	BD.HW.001		4	AEF14	Errores de monitorización (log)	VRH03	Falla de mecanismos de monitoreo		3	-	2	3	4	4	4
2	BD.HW.002	Patch Panel	4	AAI21	Manipulación de hardware y/o equipos	VRH04	Falta de capacitación y educación en seguridad de información		3	2	3	3	4	3	4
3	BD.INF.002	Orden de salida de equipos	4	AEF01	Alteración de la información	VOC08	Falta de procedimientos para el manejo de la información		2	3	-	3	4	3	4
	BD.INF.002		4	AEF09	Divulgación de información	VRH01	Carencia de toma de		3	-	-	3	4	2	3

Activo Crítico				Amenazas Potenciales		Vulnerabilidad Importantes		Analisis del Riesgo							
N°	Código del Activo	Activo	Valor del Activo	Código Amenaza	Amenaza	Código Vulnerabilidad	Vulnerabilidad	Controles existentes	Degradación			Degradación Máxima	Impacto	Probabilidad	Riesgo
									C	I	D				
							conciencia en seguridad								
4	BD.INF.003	Formato de préstamo de equipo	4	AEF01	Alteración de la información	VOC08	Falta de procedimientos para el manejo de la información		2	3	-	3	4	3	4
	BD.INF.003		4	AEF09	Divulgación de información	VRH01	Carencia de toma de conciencia en seguridad		3	-	-	3	4	2	3
5	BD.PER.001	Jefe de Unidad de Soporte	5	AEF19	Indisponibilidad del personal / Ausencia accidental	VRH05	Falta de personal para desempeñar el rol		-	-	3	3	4	4	4
6	BD.PER.002	Encargada Help Desk	4	AEF19	Indisponibilidad del personal / Ausencia accidental	VRH05	Falta de personal para desempeñar el rol		-	-	3	3	4	3	4
7	BD.SW.001	Antivirus Corporativo NOD32	4	xAEF02	Caída de aplicaciones o del sistema operativo	VOC16	Falta de registro de fallas e incidencias	se revisan los log periódicamente, pero no se genera informe	-	-	3	3	4	4	4
	ST.SW.001		4	AEF08	Difusión de software dañino (Virús, spyware, etc)	VOC23	Falta o falla de controles contra código malicioso		3	-	3	3	4	2	3
	ST.SW.001		4	AEF13	Errores de mantenimiento / actualización	VOC36	incumplimiento de las políticas para la protección	Se revisan y corrigen	2	2	2	2	3	3	3

Activo Crítico				Amenazas Potenciales		Vulnerabilidad Importantes		Analisis del Riesgo							
N°	Código del Activo	Activo	Valor del Activo	Código Amenaza	Amenaza	Código Vulnerabilidad	Vulnerabilidad	Controles existentes	Degradación			Degradación Máxima	Impacto	Probabilidad	Riesgo
									C	I	D				
					de programas (software)		de los sistemas de información								
8	ST.SW.003	Microsoft Excel	4	AAI02	Acceso no autorizado	VOC36	Incumplimiento de las políticas para la protección de los sistemas de información		3	2	3	3	[redacted]	3	[redacted]
9	ST.SER.001	Servicio Eléctrico	4	ASE01	Caída general del servicio eléctrico	VFA10	Falta o deficiencia en protección contra amenazas externas y ambientales		-	-	2	2	3	2	3

ANEXO 03
EVALUACIÓN DEL RIESGO

						CRITERIOS PARA EVALUAR LA RELEVANCIA DEL RIESGO						
N°	Código Activo	Activo	Código Amenaza	Amenaza	Riesgo	Económico	Continuidad	Legal	Imagen	Contractual	Subtotal	Total
1	ST.HW.001	Switch	AAI22	Manipulación de la configuración	4		X				1	4
2	ST.HW.001	Switch	AEF14	Errores de monitorización (log)	4		X				1	4
3	ST.HW.002	Patch Panel	AAI21	Manipulación de hardware y/o equipos	4		X				1	4
4	ST.INF.002	Orden de salida de equipos	AEF01	Alteración de la información	4		X	X			2	8
5	ST.INF.003	Formatos de préstamo de equipo	AEF01	Alteración de la información	4		X	X			2	8
6	ST.PER.001	Jefe de Unidad de Gestión de Informática	AEF19	Indisponibilidad del personal / Ausencia accidental	4		X		X		2	8
7	ST.PER.002	Encargada de Help Desk	AEF19	Indisponibilidad del personal / Ausencia accidental	4		X		X		2	8
8	ST.SW.001	Antivirus Corporativo NOD32	AEF02	Caída de aplicaciones o del sistema operativo	4		X	X	X		3	12
9	ST.SW.003	Microsoft Excel	AAI02	Acceso no autorizado	4		X		X		2	8
10	ST.SER.001	Transformador	AOI01	Avería de origen físico o lógico	4		X				1	4

Oficina Central de Informática – UNPRG	Nro. Documento: **PST-005/01**
	Confidencial

PROCESO DE SOPORTE DE TI

INFORME DE OPCIONES DE TRATAMIENTO DEL RIESGO

ÍNDICE

1. OBJETIVO

Desarrollar las opciones de tratamiento de riesgos del proceso de Soporte de TI de la Oficina Central de Informática según alcance, como resultado del Análisis y Evaluación de riesgos.

2. BASE LEGAL

ISO/IEC 27001:2007 Sistema de Gestión de la Seguridad de la Información (SGSI)-Requisitos, 4.2.1 Establecimiento del SGSI, numerales d),e),f).

3. ALCANCE

Este documento es elaborado para realizar el tratamiento del Riesgo del Proceso de Soporte de TI de la Oficina Central de Informática según el documento del Alcance del SGSI.

4. DEFINICIONES

4.1 Información: Datos que poseen significado.

4.2 Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

4.3 Integridad: Garantía de la exactitud y el contenido completo de la información. Asegurar de Proteger a la información de cualquier modificación o destrucción no autorizada.

4.4 Disponibilidad: Asegurar el acceso a la información por parte de los usuarios autorizados en el momento que ellos lo requieran.

4.5 Activo de Información: La información y su medio de soporte (por ejemplo, expediente, bases de datos) así como los activos asociados con el procesamiento de información (computadoras, red interne, aplicativos).

4.6 Clasificación de la Información
Es aquel proceso por el que se caracteriza a los diferentes tipos de información:

CLASIFICACIÓN	DESCRIPCIÓN
Información Confidencial	Información a la cual solo tienen acceso un número reducido de usuario. Si se produce un acceso no autorizado puede impactar significantemente contra la organización, clientes, personal o terceros.
Información Restringida	Información utilizada por el personal para conducir las operaciones del negocio, y que puede ser compartido con terceros en forma autorizada.
Información Pública	Información disponible para distribuir al público, siguiendo procedimientos o canales establecidos. Información de dominio público.

4.7 Tipos de Activo

Puede resultar conveniente dividir los activos de información según su estado y características propias. A modo de ejemplo, se muestran los siguientes tipos:

- **Recurso de Información**: Información que se encuentra impresa o manuscrita, tangible o intangible que se utiliza para ciertas actividades del proceso.

- **Software**: Conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina.

- **Hardware**: Corresponde al equipamiento informático (Pcs, laptops, servidores), equipos de comunicaciones y seguridad (routers, hubs, switches, redes, firewalls, IDPs, Secure Access, entre otros), medios magnéticos (cintas, CDs, y discos).

- **Servicios**: Tales como Energía Eléctrica, Agua, Red, Conexión VPN, telefonía, ente otros Estos servicios se apoyan generalmente en elementos de hardware (cables, tubos, etc.) pero los usuarios los perciben como servicios.

- **Personal**: Incluye a todo el personal involucrado en el proceso, en este caso del Proceso de Soporte de TI.

4.8 Amenaza

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Algunos ejemplos de Amenaza: Adulteración de documentos, Fuga de información, Incendio,

Terremoto, Código Malicioso, Caída Eléctrica, Falla en los Servicios de Comunicación, etc.

4.9 Vulnerabilidad

Es la debilidad de un activo o grupo de activos, que pueden ser explotadas por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.
Algunos ejemplos de vulnerabilidad: que no se cuente con personal capacitado, falta de control de privilegios del sistema, errores de programación, etc.

4.10 Control

Significa el manejo del riesgo, lo que puede incluir políticas, procedimientos, guías, prácticas, nuevo equipos o nuevas estructuras organizaciones; las cuales pueden tener naturaleza administrativa, técnica, legal o de gestión. El término Control es también utilizado como sinónimo de salvaguarda o contramedida. Los controles pueden ser preventivos, detectores, correctivos o persuasivos.

- **Los controles preventivos** sirven para que la amenaza no cumpla con su objetivo de atentar contra la seguridad del activo, por ejemplo, la delimitación del perímetro de la seguridad física.
- **Los controles detectores** son aquello que sirven para descubrir amenazas o vulnerabilidades de la seguridad de la información, por ejemplo instalar un software detector de intrusos (IDS).
- **Los controles disuasivos** sirven para que el agente de la amenaza desiste de tomar acciones que atenta contra la seguridad de la información de los activos. Un ejemplo son los procesos disciplinarios.
- **Los controles correctivos** son aquellos que se ejecutan después de un ataque contra la seguridad de la información y sirven para corregir el daño en la seguridad que ha sufrido el activo. Un ejemplo es la inclusión de cámaras de seguridad después de sufrir un robo en la organización.

4.11 Controles Existentes

Son aquellos controles que ya se encuentran implementados por la organización, previamente el análisis de Riesgo realizado.

4.12 Riesgo

Se denomina riesgo a la medida del daño probable sobre un activo. Conociendo el impacto de las amenaza sobre los activos, se deriva el riesgo sin más que tener en cuenta la probabilidad de ocurrencia de la amenaza.

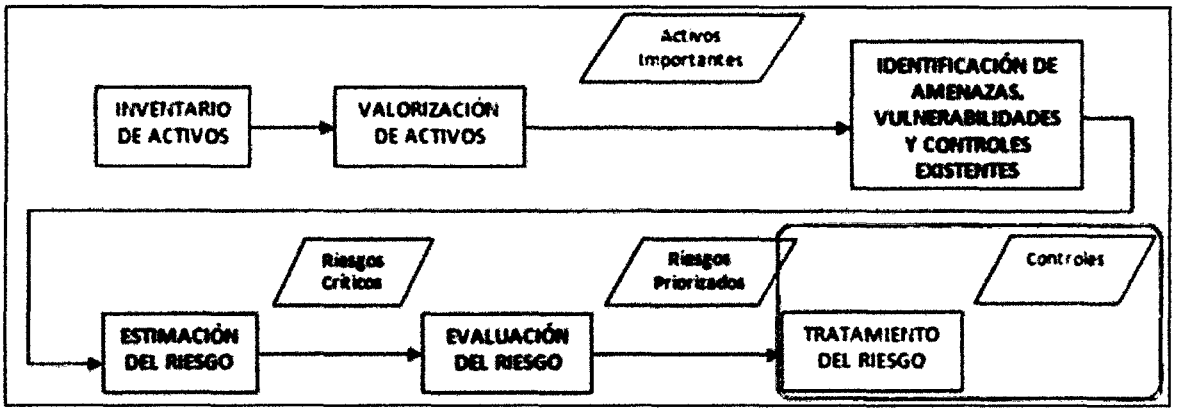
5. ABREVIATURAS

5.1 SGSI: Sistemas de Gestión de Seguridad de la Información

6. METODOLOGÍA DEL ANÁLISIS, EVALUACIÓN Y OPCIONES DE TRATAMIENTO DEL RIESGO

La metodología de Gestión del Riesgo se ha dividido en 4 partes:

i. Inventario de Activos de Información.
ii. Análisis del Riesgo.
iii. Evaluación del Riesgo.
iv. Opciones de Tratamiento del Riesgo.



7. OPCIONES DE TRATAMIENTO DEL RIESGO

Una vez efectuado el análisis y evaluación del riesgo, se debe decidir cómo tratar el riesgo basándonos en las opciones, detallas en la siguiente tabla:

Tratamiento	Descripción
Reducir	Establecer controles para atenuación (políticas, procedimientos, procesos y herramientas).
Aceptar	Aceptar el riesgo en su presente nivel debido a que no es posible realizar un tratamiento o porque éste resulta demasiado caro.
Transferir	Transferir a un tercero con capacidad financiera / especialización necesaria para administrar el riesgo adecuadamente.
Evitar	Evitar el riesgo eliminándolo de la actividad de la organización.

De lo cual se ha elaborado las opciones de tratamiento para el proceso de Soporte de TI para La Oficina Central de Informática (Anexo 01).

ANEXO 01

OPCIONES DE TRATAMIENTO DE RIESGOS

N°	Activo	Amenaza	Riesgo	Opciones de tratamiento Pre-Test	Opciones de tratamiento Pos-Test
1	Switch	Manipulación de la configuración	4	Transferir	Transferir
		Errores de mantenimiento / actualización de equipos (hardware)	3	Aceptar	Aceptar
		Errores de monitorización (log)	4	Reducir	Aceptar
2	Patch Panel	Manipulación de hardware y/o equipos	4	Transferir	Transferir
3	Orden de salida de equipos	Alteración de la información	4	Reducir	Aceptar
		Divulgación de información	3	Aceptar	Aceptar
4	Formatos de préstamo de equipo	Alteración de la información	4	Reducir	Aceptar
		Divulgación de información	3	Aceptar	Aceptar
5	Jefe de Unidad de Soporte	Indisponibilidad del personal / Ausencia accidental	4	Reducir	Aceptar
6	Encargada de Help Desk	Indisponibilidad del personal / Ausencia accidental	4	Reducir	Aceptar
7	Antivirus Corporativo NOD32	Caída de aplicaciones o del sistema operativo	4	Reducir	Aceptar

N°	Activo	Amenaza	Riesgo	Opciones de tratamiento Pre-Test	Opciones de tratamiento Pos-Test
		Difusión de software dañino (Virús, spyware, etc)	3	Aceptar	Aceptar
		Errores de mantenimiento / actualización de programas (software)	3	Aceptar	Aceptar
8	Microsoft Excel	Acceso no autorizado	4	Aceptar	Aceptar
9	Servicio Eléctrico	Caída general del servicio eléctrico	3	Aceptar	Aceptar

Oficina Central de Informática – UNPRG	Nro. Documento: **PST-004/01**
	CONFIDENCIAL

PROCESO DE SOPORTE DE TI

INFORME DEL ENUNCIADO DE APLICABILIDAD DE LOS RIESGOS

ÍNDICE

1. OBJETIVO

- Seleccionar los controles adecuados que permitan mitigar los riesgos detectados en el análisis de riesgos del Proceso de Soporte de TI de la Oficina Central de Informática.
- Preparar un Enunciado de Aplicabilidad que proporciona los controles aplicables y no aplicables para el proceso.
- Conocer qué controles existen y no existen implementados del Proceso de Soporte de TI de la Oficina Central de Informática.
- Justificar las exclusiones y proporcionar un chequeo para asegurar que ningún control haya sido omitido inadvertidamente de la ISO 27001.

2. BASE LEGAL

ISO/IEC 27001:2005Sistema de Gestión de la Seguridad de la Información (SGSI)- Requisitos, 4.2.1 Establecimiento del SGSI, numerales j).

3. DEFINICIONES

3.1Información: Datos que poseen significado.

3.2Activo de Información: La información y su medio de soporte (por ejemplo, documentos, bases de datos) así como los activos asociados conel procesamiento de información (computadoras, red internet, aplicativos).

3.3Riesgo: Se denomina riesgo a la medida del daño probable sobre un activo. Conociendo el impacto de las amenazas sobre los activos, se deriva el riesgo sin más que tener en cuenta la probabilidad de ocurrencia de la amenaza.

3.4Control

Significa el manejo del riesgo, lo que puede incluir políticas, procedimientos, guías, prácticas, nuevo equipos o nuevas estructuras organizaciones; las cuales pueden tener naturaleza administrativa, técnica, legal o de gestión. El término Control es también utilizado como sinónimo de salvaguarda o contramedida. Los controles pueden ser preventivos, detectores, correctivos o persuasivos.

- **Los controles preventivos** sirven para que la amenaza no cumpla con su objetivo de atentar contra la seguridad del activo, por ejemplo, la delimitación del perímetro de la seguridad física.
- **Los controles detectores** son aquellos que sirven para descubrir amenazas o vulnerabilidades de la seguridad de la información, por ejemplo instalar un software detector de intrusos (IDS).
- **Los controles disuasivos** sirven para que el agente de la amenaza desiste de tomar acciones que atenta contra la seguridad de la información de los activos. Un ejemplo son los procesos disciplinarios.
- **Los controles correctivos** son aquellos que se ejecutan después de un ataque contra la seguridad de la información y sirven para corregir el daño en la seguridad que ha

sufrido el activo. Un ejemplo es la inclusión de cámaras de seguridad después de sufrir un robo en la organización.

3.5Controles Existentes

Son aquellos controles que ya se encuentran implementados por la organización, previamente el análisis de Riesgo realizado.

3.6Degradación

Es el grado en que se ve afectado al activo de información, cuando una vulnerabilidad es explotada por una amenaza, tomando en cuenta los controles existentes.

3.7Impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, se deriva el impacto que estas tendrían.

3.8Probabilidad

Posibilidad de que se materialice la amenaza, es decir, que se produzca un ataque éxitos, tomando en cuenta las vulnerabilidades y los controles existentes.

3.9Riesgo

Se denomina riesgo a la medida del daño probable sobre un activo. Conociendo el impacto de las amenaza sobre los activos, se deriva el riesgo sin más que tener en cuenta la probabilidad de ocurrencia de la amenaza.

4. ABREVIATURAS

4.1SGSI: Sistemas de Gestión de Seguridad de la Información

5. DECLARACIÓN DE APLICABILIDAD

Cláusula	Sección	Objetivo de Control	¿Aplicable? SI/NO	Control Pre - Test	Control Pre - Test
5. Políticas de Seguridad	5.1	**Política de Seguridad de la Información**			
	5.1.1	Documento de la Política de Seguridad	si	No existe	Si existe
	5.1.2	Revisión de la política de seguridad de la información	si	No existe	Si existe
6.Organización de la Seguridad de la Información	6.1	**Organización interna**			
	6.1.1	Compromiso de la Gerencia con la Seguridad de Información	si	No existe	Si existe
	6.1.2	Coordinación de Seguridad de Información	si	No existe	No existe
	6.1.3	Asignación de responsabilidades para la seguridad de la información	si	No existe	No existe
	6.1.4	Proceso de Autorización para los medios de Procesamiento de la información	si	No existe	No existe
	6.1.5	Acuerdos de Confidencialidad	si	No existe	No existe
	6.1.6	Contacto entre autoridades	si	Parcial	Parcial
	6.1.7	Contacto con grupos de Interés especial	si	No existe||	No existe
	6.1.8	Revisión independiente de Seguridad de Información	si	No existe	No existe
	6.2	**Entidades Externas**			
	6.2.1	Identificación de riesgos por el acceso de terceros	si	No existe	No existe

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	6.2.2	Tratamiento de la Seguridad en relación con Clientes	si	No existe	No existe
	6.2.3	Requisitos de Seguridad en contratos con Terceros	si	No existe	No existe
7.Gestión de Activos	**7.1**	**Responsabilidad por los activos**			
	7.1.1	Inventario de activos	si	Parcial	Si existe
	7.1.2	Propiedad de los activos	si	No existe	Si existe
	7.1.3	Uso aceptable de los activos	si	No existe	No existe
	7.2	**Clasificación de la Información**			
	7.2.1	Lineamientos de clasificación	si	No existe	Si existe
	7.2.2	Etiquetado y manejo de la información	si	No existe	No existe
8.Seguridad de Recursos Humanos	**8.1**	**Antes del Empleo**			
	8.1.1	Roles y Responsabilidades	si	Parcial	Si existe
	8.1.2	Selección	si	No existe	No existe
	8.1.3	Términos y condiciones de empleo	si	Si existe	Si existe
	8.2	**Durante el empleo**			
	8.2.1	Responsabilidades de gestión	si	No existe	No existe
	8.2.2	Capacitación y educación en seguridad de la información	si	No existe	Si existe
	8.2.3	Proceso disciplinario	si	No existe	Si existe
	8.3	**Terminación o cambio del empleo**			

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	8.3.1	Responsabilidades de terminación	si	No existe	No existe
	8.3.2	Devolución de activos	si	No existe	No existe
	8.3.3	Eliminación de derechos de acceso	si	Si existe	Si existe
9.Seguridad Física y Ambiental	9.1	**Áreas Seguras**			
	9.1.1	Perímetro de seguridad física	si	Si existe	Si existe
	9.1.2	Controles de entrada físicos	si	parcial	parcial
	9.1.3	Seguridad de oficinas	si	No existe	No existe
	9.1.4	Protección contra amenazas externas y ambientales	si	No existe	No existe
	9.1.5	Trabajo en áreas seguras	si	No existe	No existe
	9.1.6	Áreas de acceso público, entrega y carga	si	No existe	No existe
	9.2	**Seguridad de equipos**			
	9.2.1	Ubicación y protección del equipo	si	No existe	No existe
	9.2.2	Servicios de Soporte (instalación de Suministros)	si	No existe	No existe
	9.2.3	Seguridad en el cableado	si	Si existe	Si existe
	9.2.4	Mantenimiento de equipo	si	Si existe	Si existe

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	9.2.5	Seguridad del equipo fuera del local	si	No existe	No existe
	9.2.6	Eliminación seguro o re-uso del equipo	si	No existe	Si existe
	9.2.7	Traslado de Propiedad	si	Si existe	Si existe
10.Gestión de Comunicaciones y operaciones	**10.1**	**Procedimiento y responsabilidades operacionales**			
	10.1.1	Documento de Procedimientos Operativos	si	No existe	No existe
	10.1.2	Gestión de cambio	si	No existe	No existe
	10.1.3	Segregación de deberes	si	parcial	parcial
	10.1.4	Separación de los medios de desarrollo y operacionales	si	Si existe	Si existe
	10.2	**Gestión de la entrega del servicio de terceros**			
	10.2.1	Prestación del servicio	si	No existe	No existe
	10.2.2	Monitoreo y revisión de los servicios de terceros	si	No existe	No existe
	10.2.3	Manejar los cambios en los servicios de terceros	si	No existe	No existe
	10.3	**Planificación y Aceptación del Sistema**			
	10.3.1	Gestión de la capacidad	si	No existe	No existe
	10.3.2	Aceptación del sistema	si	No existe	No existe

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	10.4	**Protección contra software malicioso y código móvil**			
	10.4.1	Controles contra software malicioso	si	Si existe	Si existe
	10.4.2	Controles contra Código Móvil	no		
	10.5	**Respaldo**			
	10.5.1	Respaldo de la Información	si	Parcial	Si existe
	10.6	**Gestión de seguridad de redes**			
	10.6.1	Controles de red	si	No existe	No existe
	10.6.2	Seguridad de los servicios de red	si	No existe	No existe
	10.7	**Gestión de Medios**			
	10.7.1	Gestión de los medios Removibles	si	No existe	No existe
	10.7.2	Eliminación de medios	si	No existe	No existe
	10.7.3	Procedimientos de manejo de la información	si	No existe	Si existe
	10.7.4	Seguridad de documentación del sistema	si	Si existe	Si existe
	10.8	**Intercambio de Información**			
	10.8.1	Procedimiento y políticas de información y software	si	No existe	No existe
	10.8.2	Acuerdos de intercambio	si	No existe	No existe

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	10.8.3	Medios físicos en tránsito	si	No existe	No existe
	10.8.4	Mensajeria Electrónica	si	No existe	No existe
	10.8.5	Sistemas de información comercial	no		
	10.9	**Servicios de comercio electrónico**			
	10.9.1	Comercio electrónico	no		
	10.9.2	Transacciones en línea	no		
	10.9.3	Información disponible públicamente	si	No existe	No existe
	10.10.	**Monitoreo**			
	10.10.1	Registro de auditoria	si	No existe	No existe
	10.10.2	Uso del sistema de monitoreo	si	No existe	Si existe
	10.10.3	Protección de la información del registro	si	No existe	No existe
	10.10.4	Registros del administrador y operador	si	No existe	Si existe
	10.10.5	Registro de fallas	si	No existe	No existe
	10.10.6	Sincronización de reloj	si	No existe	No existe
11.Controles de acceso	**11.1**	**Requisitos del Negocio para el Control de Accesos**			

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	11.1.1	Políticas de Control de Accesos	si	No existe	No existe
	11.2	**Gestión del acceso del usuario**			
	11.2.1	Inscripción del usuario	si	No existe	No existe
	11.2.2	Gestión de privilegios	si	No existe	Si existe
	11.2.3	Gestión de clave del usuario	si	No existe	No existe
	11.2.4	Revisión de los derechos de acceso del usuario	si	No existe	No existe
	11.3	**Responsabilidades del usuario**			
	11.3.1	Uso de contraseñas	si	parcial	parcial
	11.3.2	Equipo de usuario desatendido	si	No existe	No existe
	11.3.3	Política de pantalla y escritorio limpio	si	No existe	No existe
	11.4	**Controles de Acceso a redes**			
	11.4.1	Políticas sobre el uso de servicios en red	si	Si existe	Si existe
	11.4.2	Autenticación del usuario para conexiones externas	no		
	11.4.3	Identificación del equipo en red	si	Si existe	Si existe

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	11.4.4	Protección del puerto de diagnóstico remoto	si	Si existe	Si existe
	11.4.5	Segregación en redes	si	Si existe	Si existe
	11.4.6	Control de conexión de redes	si	No existe	No existe
	11.4.7	Control de enrutamiento de redes	si	Si existe	Si existe
	11.5	**Control de Acceso al Sistema Operativo**			
	11.5.1	Procedimiento de inicio de sesión	si	Si existe	Si existe
	11.5.2	Identificación y autenticación de usuarios	si	Si existe	Si existe
	11.5.3	Sistema de gestión de claves	si	No existe	No existe
	11.5.4	Uso de utilidades del sistema	si	No existe	No existe
	11.5.5	Sesión inactiva	si	No existe	No existe
	11.5.6	Limitación de tiempo de conexión	si	No existe	No existe
	11.6	**Control de Acceso a las Aplicaciones**			
	11.6.1	Restricción al acceso a la información	si	No existe	No existe

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	11.6.2	Aislamiento del sistema sensible	si	No existe	Si existe
	11.7	**Computación móvil y tele- trabajo**			
	11.7.1	Computación móvil y comunicaciones	si	No existe	No existe
	11.7.2	Tele-trabajo	no		
12.Adquisición Desarrollo y Mantenimientos de sistemas de información	**12.1**	**Requerimientos de seguridad de los sistemas**			
	12.1.1	Análisis y especificación de los requerimientos de seguridad	si	Si existe	Si existe
	12.2	**Procesamiento Correcto de las Aplicaciones**			
	12.2.1	Validación de los Datos de Entrada	si	Si existe	Si existe
	12.2.2	Control de procesamiento interno	si	Si existe	Si existe
	12.2.3	Integridad del mensaje	si	Si existe	Si existe
	12.2.4	Validación de data de output	si	Si existe	Si existe
	12.3	**Controles Criptográficos**			
	12.3.1	Política sobre el Uso de Controles Criptográficos	si	No existe	No existe
	12.3.2	Gestión clave	si	No existe	No existe
	12.4	**Seguridad de los Archivos del Sistema**			

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	12.4.1	Control de software operacional	si	No existe	No existe
	12.4.2	Protección de la data de prueba del sistema	si	No existe	No existe
	12.4.3	Control de acceso al código fuente del programa	si	Si existe	Si existe
	12.5	**Seguridad en los procesos de desarrollo y soporte**			
	12.5.1	Procedimientos de control de cambios	si	No existe	No existe
	12.5.2	Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo	si	No existe	No existe
	12.5.3	Restricciones a los cambios en los paquetes de software	si	No existe	No existe
	12.5.4	Fugas de información	si	No existe	No existe
	12.5.5	Desarrollo de software contratado externamente	si	No existe	No existe
	12.6	**Gestión de la Vulnerabilidad Técnica**			
	12.6.1	Control de las Vulnerabilidades técnicas	si	No existe	No existe
13.Gestión de Incidentes de Seguridad de la	**13.1**	**Notificación de eventos y puntos débiles de la seguridad de la información**			
	13.1.1	Notificación de los eventos de seguridad de la información	si	No existe	Si existe

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
Información	13.1.2	Notificación de puntos débiles de la seguridad	si	No existe	No existe
	13.2	**Gestión de incidentes de la seguridad de la información**			
	13.2.1	Responsabilidades y procedimientos	si	No existe	No existe
	13.2.2	Aprendizaje de los incidentes de seguridad de la información	si	No existe	Si existe
	13.2.3	Recopilación de evidencias	si	No existe	No existe
14.Gestión de la Continuidad del Negocio	14.1	**Aspectos de seguridad de la información en la gestión la continuidad del negocio**			
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	si	No existe	No existe
	14.1.2	Continuidad del negocio y evaluación de riesgos	si	No existe	No existe
	14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.	si	Parcial	parcial
	14.1.4	Marco de referencia para la planificación de la continuidad del negocio.	si	No existe	No existe
	14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.	si	No existe	No existe
15.Cumplimiento	15.1	**Cumplimiento de los requisitos legales**			

Cláusula	Sección	Objetivo de Control	¿Aplicable?	Control Pre - Test	Control Pre - Test
	15.1.1	Identificación de la legislación aplicable.	si	No existe	No existe
	15.1.2	Derechos de propiedad intelectual (DPI).	si	No existe	No existe
	15.1.3	Protección de los registros de la organización.	si	No existe	No existe
	15.1.4	Protección de datos y privacidad de la información personal	si	No existe	No existe
	15.1.5	Prevención del uso indebido de las instalaciones de procesamiento de la información.	si	No existe	No existe
	15.1.6	Regulación de los controles criptográficos	si	No existe	No existe
	15.2	**Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico**			
	15.2.1	Cumplimiento de las políticas y normas de seguridad	si	No existe	No existe
	15.2.2	Comprobación del cumplimiento técnico	si	No existe	No existe
	15.3	**Consideraciones de la auditoria de los sistemas de información**			
	15.3.1	Controles de auditoría de los sistemas de información.	si	No existe	No existe
	15.3.2	Protección de la herramientas de auditoría de los sistemas de información	si	Si existe	Si existe

Oficina Central de Informática – UNPRG	Nro. Documento: **PST-006/01** **CONFIDENCIAL**

PROCESO DE SOPORTE DE TI

PLAN DE TRATAMIENTO DE RIESGOS DEL PROCESO DE SOPORTE DE TI

ÍNDICE

1. OBJETIVOS

Con el Plan de Tratamiento de Riesgos se establece un cronograma de actividades para cumplir con la implementación de los controles seleccionados de la norma ISO/IEC 27001 de los riesgos a tratar.

Estos controles fueron seleccionados como parte del Informe del Enunciado de Aplicabilidad, con el objetivo de proteger los activos de la información más importantes en el Proceso de Soporte de TI de acuerdo a los resultados del Análisis de Riesgos.

Después de la selección de controles se ha determinado las acciones de gestión de acuerdo al grupo de procedimiento y la secuencia de implementación que es materializado en el Cronograma de duración de la Implementación (Anexo 1) donde se asigna los tiempos en días de la duración de la ejecución de cada control.

El objetivo principal es formular el plan de tratamiento de riesgo para su respectiva implementación según la ISO/IEC 27001.

2. REFERENCIAS

- **Activo:** Cualquier cosa que tenga valor para la organización.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **ISO/IEC 27001:2005** Tecnología de Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información - Requerimientos.

3. SUPUESTOS DEL PLAN

- Los controles de la norma ISO/IEC 27001 fueron seleccionados con el fin de que ayuden a mitigar los 10 riesgos detectados en el Informe de Análisis, evaluación.

- Este Tratamiento de Riesgos se enfoca en la implantación de controles de la norma ISO/IEC 27001:2005, con el fin de fijar una base procedimental para la seguridad de la información dentro del Proceso de Soporte de TI.

- Los procedimientos de control se irán generando y presentado de manera progresiva para revisión y aprobación.

- En todos los controles de la ISO/IEC 27001:2005 a implementar se van a dar prioridad para dirigir a los riesgos identificados en el análisis.

4. LISTA DE CONTROLES ISO SELECCIONADOS

La lista de 127 controles seleccionados de la norma ISO/IEC 27001:2005 para el Proceso de Soporte de TI son los que se presentan en el siguiente cuadro:

TABLA 4.1 Controles Seleccionados

Controles del "Controles A"(ISO/IEC 27001:2005)		
Cláusula	**Sección**	**Objetivo de Control**
5. Políticas de Seguridad	**5.1**	**Política de Seguridad de la Información**
	5.1.1	Documento de la Política de Seguridad
	5.1.2	Revisión de la política de seguridad de la información
6.Organización de la Seguridad de la Información	**6.1**	**Organización interna**
	6.1.1	Compromiso de la Gerencia con la Seguridad de Información
	6.1.2	Coordinación de Seguridad de Infomación
	6.1.3	Asignación de responsabilidades para la seguridad de la información
	6.1.4	Proceso de Autorización para los medios de Procesamiento de la información
	6.1.5	Acuerdos de Confidencialidad
	6.1.6	Contacto entre autoridades
	6.1.7	Contacto con grupos de Interés especial
	6.1.8	Revisión independiente de Seguridad de Información
	6.2	**Entidades Externas**
	6.2.1	Identificación de riesgos por el acceso de terceros
	6.2.2	Tratamiento de la Seguridad en relación con Clientes
	6.2.3	Requisitos de Seguridad en contratos con Terceros
7.Gestión de Activos	**7.1**	**Responsabilidad por los activos**
	7.1.1	Inventario de activos
	7.1.2	Propiedad de los activos
	7.1.3	Uso aceptable de los activos
	7.2	**Clasificación de la Información**
	7.2.1	Lineamientos de clasificación
	7.2.2	Etiquetado y manejo de la información
8.Seguridad de	**8.1**	**Antes del Empleo**

Controles del "Controles A"(ISO/IEC 27001:2005)		
Cláusula	**Sección**	**Objetivo de Control**
Recursos Humanos	8.1.1	Roles y Responsabilidades
	8.1.2	Selección
	8.1.3	Terminos y condiciones de empleo
	8.2	**Durante el empleo**
	8.2.1	Responsabilidades de gestión
	8.2.2	Capacitación y educación en seguridad de la información
	8.2.3	Proceso disciplinario
	8.3	**Terminación o cambio del empleo**
	8.3.1	Responsabilidades de terminación
	8.3.2	Devolución de activos
	8.3.3	Eliminación de derechos de acceso
9.Seguridad Física y Ambiental	**9.1**	**Areas Seguras**
	9.1.1	Perímetro de seguridad física
	9.1.2	Controles de entrada físicos
	9.1.3	Seguridad de oficinas
	9.1.4	Protección contra amenazas externas y ambientales
	9.1.5	Trabajo en áreas seguras
	9.1.6	Areas de acceso público, entrega y carga
	9.2	**Seguridad de equipos**
	9.2.1	Ubicación y protección del equipo
	9.2.2	Servicios de Soporte (instalación de Suministros)
	9.2.3	Seguridad en el cableado
	9.2.4	Mantenimiento de equipo
	9.2.5	Seguridad del equipo fuera del local
	9.2.6	Eliminación seguro o re-uso del equipo
	9.2.7	Traslado de Propiedad
10.Gestión de Comunicaciones y operaciones	**10.1**	**Procedimiento y responsabilidades operacionales**
	10.1.1	Documento de Procedimientos Operativos
	10.1.2	Gestión de cambio
	10.1.3	Segregación de deberes
	10.1.4	Separación de los medios de desarrollo y operacionales
	10.2	**Gestión de la entrega del servicio de terceros**
	10.2.1	Prestación del servicio
	10.2.2	Monitoreo y revisión de los servicios de terceros
	10.2.3	Manejar los cambios en los servicios de terceros

Controles del "Controles A" (ISO/IEC 27001:2005)		
Cláusula	**Sección**	**Objetivo de Control**
	10.3	**Planificación y Aceptación del Sistema**
	10.3.1	Gestión de la capacidad
	10.3.2	Aceptación del sistema
	10.4	**Protección contra software malicioso y código móvil**
	10.4.1	Controles contra software malicioso
	10.5	**Respaldo**
	10.5.1	Respaldo de la Información
	10.6	**Gestión de seguridad de redes**
	10.6.1	Controles de red
	10.6.2	Seguridad de los servicios de red
	10.7	**Gestión de Medios**
	10.7.1	Gestión de los medios Removibles
	10.7.2	Eliminación de medios
	10.7.3	Procedimientos de manejo de la información
	10.7.4	Seguridad de documentación del sistema
	10.8	**Intercambio de Información**
	10.8.1	Procedimiento y políticas de información y software
	10.8.2	Acuerdos de intercambio
	10.8.3	Medios físicos en tránsito
	10.8.4	Mensajeria Electrónica
	10.9	**Servicios de comercio electrónico**
	10.9.3	Información disponible públicamente
	10.10.	**Monitoreo**
	10.10.1	Registro de auditoria
	10.10.2	Uso del sistema de monitoreo
	10.10.3	Protección de la información del registro
	10.10.4	Registros del administrador y operador
	10.10.5	Registro de fallas
	10.10.6	Sincronización de reloj
11.Controles de acceso	**11.1**	**Requisitos del Negocio para el Control de Accesos**
	11.1.1	Políticas de Control de Accesos
	11.2	**Gestión del acceso del usuario**
	11.2.1	Inscripción del usuario
	11.2.2	Gestión de privilegios
	11.2.3	Gestión de clave del usuario

Controles del "Controles A"(ISO/IEC 27001:2005)		
Cláusula	**Sección**	**Objetivo de Control**
	11.2.4	Revisión de los derechos de acceso del usuario
	11.3	**Responsabilidades del usuario**
	11.3.1	Uso de contraseñas
	11.3.2	Equipo de usuario desatendido
	11.3.3	Política de pantalla y escritorio limpio
	11.4	**Controles de Acceso a redes**
	11.4.1	Políticas sobre el uso de servicios en red
	11.4.3	Identificación del equipo en red
	11.4.4	Protección del puerto de diagnóstico remoto
	11.4.5	Segregación en redes
	11.4.6	Control de conexión de redes
	11.4.7	Control de enrutamiento de redes
	11.5	**Control de Acceso al Sistema Operativo**
	11.5.1	Procedimiento de inicio de sesión
	11.5.2	Identificación y autenticación de usuarios
	11.5.3	Sistema de gestión de claves
	11.5.4	Uso de utilidades del sistema
	11.5.5	Sesión inactiva
	11.5.6	Limitación de tiempo de conexión
	11.6	**Control de Acceso a las Aplicaciones**
	11.6.1	Restricción al acceso a la información
	11.6.2	Aislamiento del sistema sensible
	11.7	**Computación móvil y tele- trabajo**
	11.7.1	Computación móvil y comunicaciones
12.Adquisición Desarrollo y Mantenimientos de sistemas de información	**12.1**	**Requerimientos de seguridad de los sistemas**
	12.1.1	Análisis y especificación de los requerimientos de seguridad
	12.2	**Procesamiento Correcto de las Aplicaciones**
	12.2.1	Validación de los Datos de Entrada
	12.2.2	Control de procesamiento interno
	12.2.3	Integridad del mensaje
	12.2.4	Validación de data de output
	12.3	**Controles Criptográficos**
	12.3.1	Política sobre el Uso de Controles Criptográficos
	12.3.2	Gestión clave
	12.4	**Seguridad de los Archivos del Sistema**

Controles del "Controles A"(ISO/IEC 27001:2005)		
Cláusula	**Sección**	**Objetivo de Control**
	12.4.1	Control de software operacional
	12.4.2	Protección de la data de prueba del sistema
	12.4.3	Control de acceso al código fuente del programa
	12.5	**Seguridad en los procesos de desarrollo y soporte**
	12.5.1	Procedimientos de control de cambios
	12.5.2	Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo
	12.5.3	Restricciones a los cambios en los paquetes de software
	12.5.4	Fugas de información
	12.5.5	Desarrollo de software contratado externamente
	12.6	**Gestión de la Vulnerabilidad Técnica**
	12.6.1	Control de las Vulnerabilidades técnicas
13.Gestión de Incidentes de Seguridad de la Información	**13.1**	**Notificación de eventos y puntos débiles de la seguridad de la información**
	13.1.1	Notificación de los eventos de seguridad de la información
	13.1.2	Notificación de puntos débiles de la seguridad
	13.2	**Gestión de incidentes de la seguridad de la información**
	13.2.1	Responsabilidades y procedimientos
	13.2.2	Aprendizaje de los incidentes de seguridad de la información
	13.2.3	Recopilación de evidencias
14.Gestión de la Continuidad del Negocio	**14.1**	**Aspectos de seguridad de la información en la gestión la continuidad del negocio**
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
	14.1.2	Continuidad del negocio y evaluación de riesgos
	14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.
	14.1.4	Marco de referencia para la planificación de la continuidad del negocio.
	14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.
15.Cumplimiento	**15.1**	**Cumplimiento de los requisitos legales**
	15.1.1	Identificación de la legislación aplicable.
	15.1.2	Derechos de propiedad intelectual (DPI).
	15.1.3	Protección de los registros de la organización.
	15.1.4	Protección de datos y privacidad de la información personal
	15.1.5	Prevención del uso indebido de las instalaciones de procesamiento de la información.
	15.1.6	Regulación de los controles criptográficos
	15.2	**Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico**
	15.2.1	Cumplimiento de las políticas y normas de seguridad
	15.2.2	Comprobación del cumplimiento técnico

Controles del "Controles A"(ISO/IEC 27001:2005)		
Cláusula	Sección	Objetivo de Control
	15.3	Consideraciones de la auditoria de los sistemas de información
	15.3.1	Controles de auditoría de los sistemas de información.
	15.3.2	Protección de la herramientas de auditoría de los sistemas de información

5. GRUPOS DE PROCEDIMIENTOS DE SEGURIDAD

5.1 Grupos de Procedimientos

La implantación de los controles ISO en el Proceso de Soporte de TI se realizará por medio de Procedimientos de Seguridad. Estos procedimientos en varios casos estan soportados con herramientas tecnologicas tales como software, hardware u otro que ayudan a cumplir con lo requerido por el estandar, con la finalidad de ser más eficiente y eficaz.

Para tal fin se han diseñado 08 grupos de procedimientos, con los cuales se procederá a implementar los 81 controles de la Norma ISO. Cada grupo de procedimientos cubre una cierta cantidad de controles.

Los 08 grupos de procedimientos de seguridad son los siguientes:

GRUPO 1: Gestión de la Seguridad de la Información

GRUPO 2: Seguridad con Recursos Humanos

GRUPO 3: Seguridad con Terceros

GRUPO 4: Seguridad del Entorno

GRUPO 5: Seguridad de los Activos de Información

GRUPO 6: Gestión de Operaciones de Sistemas

GRUPO 7: Control de Accesos

GRUPO 8: Gestión de Incidentes y Continuidad Operativa

5.2 Ventajas del esquema de Grupos de Procedimientos

Se decidió realizar la implementación de los controles a través de Grupos de Procedimientos, por los siguientes motivos:

- Con los Grupos de Procedimientos se pueden agrupar y consolidar controles ISO que traten sobre temas similares, pero que pertenecen a diferentes Dominios de la norma. Por

ejemplo, el grupo de Procedimientos "5.7. Instalación de equipos y software", consolida algunos controles de los dominios 6 (Seguridad fisica), 9 (Operaciones) y 15 (Normativa y Legal). Esto permite evitar una multiplicación de procedimientos, que puede resultar contraproducente al momento de su aplicación.

- Con los Grupos de Procedimientos también se cumple con el objetivo de facilitar el aprendizaje y la implementación de los procedimientos a sus futuros usuarios y ejecutores, que no necesariamente tienen un conocimiento especializado de la norma ISO/IEC 27001:2005.

En la siguiente tabla se presentan los 29 procedimientos y los controles ISO contemplados:

Tabla 5.1 Procedimientos versus Controles ISO

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO
1. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Politicas del SGSI y objetivos	5.1.1	Politicas de Seguridad de Gestión de Seguridad de la Información
	Organización Interna de la Seguridad de la Información	6.1.1	Compromiso de la Dirección con la Seguridad de la Información
		6.1.2	Coordinación de la Seguridad de Información
		6.1.3	Asignación de las responsabilidades de la Seguridad de Información
		7.1.2	Propiedad de los activos.
		6.1.7	Contactos con grupos interesados
2. SEGURIDAD CON RECURSOS HUMANOS	Seguridad en la Selección de Personal	6.1.5	Acuerdos de Confidencialidad
		8.1.1	Roles y Responsabilidades
		8.1.2	Selección de personal.
		8.1.3	Términos y condiciones de la relación laboral.
	Concienciación y Capacitación en Seguridad de la Información	8.2.1	Responsabilidades de la Gerencia.
		8.2.2	Concienciación, educación y formación en la Seguridad de Información.
	Proceso Disciplinario	8.2.3	Proceso Disciplinario.
		15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información.
	Seguridad en la Finalización de la Relación	8.3.1	Responsabilidades en la desvinculación

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO
	Laboral	8.3.2	Devolución de activos.
		8.3.3	Remoción de los derechos de acceso.
3. SEGURIDAD CON TERCEROS	Consideraciones de Seguridad con partes externas	6.2.1	Identificación de riesgos relacionados con partes externas
		6.2.2	Tener en cuenta la seguridad cuando se trata con clientes
		6.2.3	Tratamiento de seguridad en los acuerdos de terceras partes
4. SEGURIDAD DEL ENTORNO	Seguridad Física y Ambiental	9.1.1	Perímetro de la Seguridad Física
		9.1.2	Controles de acceso físico
	Trabajo seguro en Oficinas	9.1.3	Seguridad de oficinas, despachos e instalaciones
		9.1.5	Trabajo en Areas Seguras
5. SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN	Clasificación y Manejo Seguro de la Información	7.1.1	Inventario de activos.
		7.1.2	Propiedad de los activos.
		7.2.1	Guías de clasificación.
	Análisis de Riesgos y Plan de Tratamiento	6.2.1	Identificación de riesgos relacionados con partes externas
	Uso Aceptable de los recursos de Información	7.1.3	Uso adecuado de los activos.
		7.2.2	Etiquetado y manejo de la información
		10.7.3	Procedimiento en el manejo de la información
		11.3.2	Equipo desatendido
		11.3.3	Política de escritorio y pantalla limpios
		10.1.1	Procedimientos de operación documentados
		10.7.4	Seguridad de la documentación de sistemas

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO
		10.8.5	Sistemas de información del negocio
		15.1.3	Protección de los registros de la organización.
		15.1.4	Proteccion de datos y de la privacidad de la información de las personas
		15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información.
	Uso Aceptable de los recursos de Información	7.1.3	Uso adecuado de los activos.
		11.3.2	Equipo de usuario desatendido
		11.3.3	Política de escritorio y pantalla limpios
		15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información.
	Intercambio de Información.	9.2.7	Retiro de bienes
	Seguridad en la Entrega, Retiro y Carga de Documentos.	10.8.3	Medios físicos en tránsito
	Seguridad en el Re Uso o Eliminación de Equipos Informáticos y Medios de Almacenamiento	10.7.2	Eliminación de los medios
		9.2.6	Seguridad en la reutilización o eliminación de los equipos
	Procedimiento de Instalación de Equipos	9.2.1	Ubicación y protección de los equipos
		6.1.4	Proceso de autorización para las instalaciones de procesamiento de la información

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO
		15.1.2	Derechos de propiedad intelectual (DPI)
	Mantenimiento preventivo y Correctivo	9.2.4	Mantenimiento de los equipos
		10.10.5	Registro de fallas
	Retiro de Activos de Información (Equipos de Computo)	9.2.7	Retiro de bienes
		10.8.3	Medios físicos en tránsito
6: GESTIÓN DE OPERACIONES DE SISTEMAS	Acuerdo de Uso de Dispositivos removibles y Cámaras digitales	10.7.1	Gestión de los medios removibles
	Respaldo y Restauración de la Información.	10.5.1	Respaldo (back-up) de la información
	Uso Aceptable de los recursos de Información	10.3.2	Aceptación de sistemas
		10.10.1	Registro de Auditoría
		10.10.2	Monitoreo del uso del sistema
		10.10.3	Protección de la información del registro
		10.10.4	Registro de administradores y operadores
		10.10.6	Sincronizaqción de relojes
		12.6.1	Control de las vulnerabilidades
		13.1.1	Reporte de eventos de la seguridad de información.
		15.3.1	Control de auditoria de los sistemas de información
		15.3.2	Proteccion de las herramientas de auditoria de los sistemas de información

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO
	Control de Cambios en los Sistemas y recursos de TI	10.1.2	Gestión de cambios
	Intercambio de información	10.8.1	Politicas y procedimiento de intercambio de información
		10.8.2	Acuerdos de intercambio
7. CONTROL DE ACCESOS	Administración de los Derechos de Acceso de los Usuarios	11.1.1	Política de control de acceso
		11.2.1	Registro de usuarios
		11.2.2	Gestión de privilegios
		11.2.4	Revisión de los derechos de acceso de los usuarios
	Uso de contraseñas	11.3.1	Uso de contraseñas
		11.2.3	Gestión de contraseñas de usuario
		11.5.3	Sistema de gestion de contraseñas
	Administración de los Derechos de Acceso de Usuarios.	11.4.1	Políticas sobre el uso de servicios en red
		11.4.3	Identificación de redes en la red
		11.4.4	Protección del diagnostico remoto y de la configuración de puerto
		11.4.5	Segregación en redes
		11.4.6	Control de conexión de red
		11.4.7	Control de direccionamiento de la red
	Uso Aceptable de los Recursos Informáticos	11.5.1	Procedimiento de conexión segura
		11.5.2	Identificación y autenticación de usuario

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO
		11.5.4	Uso de utilitarios (utilities) del sistema
		11.5.5	Sesión inactiva
		11.5.6	Limitacion del tiempo de conexión
8. GESTION DE INCIDENTES Y CONTINUIDAD DE NEGOCIO	Gestión de Incidentes en Seguridad de la Información	13.2.1	Responsabilidades y procedimientos.
		13.2.3	Recolección de evidencia
		6.1.6	Contacto con autoridades

6. SECUENCIA DE IMPLEMENTACIÓN

6.1 Secuencia de Implementación de los Grupos de Procedimientos

La secuencia de implementación de los grupos de procedimientos se puede apreciar en el **Anexo 01**. Dicha secuencia tomó en cuenta el nivel crítico de los procedimientos por implementar, así como el nivel de desarrollo del sistema de seguridad.

Las fechas fin que se muestran en el gráfico para cada grupo de procedimientos corresponden al momento de la entrega del grupo de procedimientos para su revisión y aprobación.

6.2 Grupo de Actividades

Dentro de la implementación de cada procedimiento se llevarán a cabo las siguientes actividades:

1. Elaborar el esquema del procedimiento:
   - Redactar el esquema del procedimiento
2. Redactar el Procedimiento
   - Reunión del Equipo SGSI con personal de la Unidad de Soporte.
   - Redacción del Procedimiento (1)
   - Reunión del Equipo SGSI con personal del Proceso de Soporte de TI (cuando sea necesario)
   - Redacción del Procedimiento (2) con las observaciones corregidas.
3. Diseñar las métricas del Procedimiento
4. Revisar y Aprobar el Grupo de Procedimientos:
   - Impresión y Envío del Grupo de Procedimientos
   - Revisión de la documentación
   - Actualización de la documentación
   - Aprobación del Grupo de Procedimientos.
5. Difundir y capacitar sobre el Grupo de Procedimientos:
   - Elaboración del plan de capacitación
   - Elaboración de los documentos de capacitación
   - Coordinación de la capacitación (lugar, recursos, convocatoria)

- Realización de la capacitación
- Elaboración del Acta de Capacitación

Notas:

- En algunos procedimientos se requerirá coordinar activamente con personal de la Oficina Central de Informática en la redacción de procedimientos
- El envío de procedimiento para su revisión y aprobación se realizará por Grupos de Procedimientos. De igual manera se agrupará la difusión y capacitación, es decir, por Grupos de Procedimientos.
- Paralelamente a la redacción de los Grupos de Procedimientos, el equipo del Proyecto SGSI puede redactar, cuando se juzgue necesario, informes que contengan planteamientos y sugerencias al Proceso de Sopote de TI de datos sobre medidas alternativas que podrían servir para mitigar los riesgos existentes.
- La ejecución y el control del procedimiento implementado será visto por los responsables que se asignarán en los procedimientos.
- En el momento de la implementacion de los controles y si fuese el caso se va a plantear o sugerir otros controles como parte de la mejora continua y que estos generaran nuevos proyectos con responsables.

7. CUADRO DE RIESGOS RESIDUALES

El tratamiento de los riesgos es la mitigación del mismo mediante la implementación de los controles ya seleccionados, como se indico anteriormente estos controles van a ser dirigidos a los riesgos, por ejemplo el riesgo Manipulación de los equipos Switch o Servidores con nivel 4 se esta implementando controles controles especifícos como el Uso del Sistema de Monitoreo, Roles y responsabilidades, , análisis de vulnerabilidades del equipo, entre otras, considerando el nivel de madurez definimos que la implementación de estos controles van a generar un riesgo residual de 2.

En esta primera fase se esta considerando bajar los niveles de los riesgos identificados, es necesario indicar que la implementar controles en general o específico no solo mitigan los riesgos identificados sino otros que no estan contemplados para su tratamiento.

Se adjunta un cuadro en el **Anexo 02** donde se detalla los riesgos, los controles a implementar, el nivel de riesgo actual y el riesgo residual, para determinar este nivel se requiere identificar la cantidad de controles especificos.

Anexo 01

Cronograma de la Implementación – Resultado del Enunciado de Aplicabilidad

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO	FECHA DE INICIO	FECHA DE FIN	ESTADO
1. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Politicas del SGSI y objetivos	5.1.1	Politicas de Seguridad de Gestión de Seguridad de la Información	08/08/2014	13/08/2014	Terminado
	Organización Interna de la Seguridad de la Información	6.1.1	Compromiso de la Dirección con la Seguridad de la Información	28/12/2014	04/01/2015	Programado
		6.1.2	Coordinación de la Seguridad de Información			
		6.1.3	Asignación de las responsabilidades de la Seguridad de Información			
		7.1.2	Propiedad de los activos.			
		6.1.7	Contactos con grupos interesados			
2. SEGURIDAD CON RECURSOS HUMANOS	Seguridad en la Selección de Personal	6.1.5	Acuerdos de Confidencialidad	07/01/2015	11/01/2015	Programado
		8.1.1	Roles y Responsabilidades			
		8.1.2	Selección de personal.			
		8.1.3	Términos y condiciones de la relación laboral.			
	Concienciación y Capacitación en Seguridad de la Información	8.2.1	Responsabilidades de la Gerencia.	14/01/2015	18/01/2015	Programado
		8.2.2	Concienciación, educación y formación en la Seguridad de Información.			
	Proceso Disciplinario	8.2.3	Proceso Disciplinario.	21/01/2015	25/01/2015	Programado
		15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información.			

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO	FECHA DE INICIO	FECHA DE FIN	ESTADO
	Seguridad en la Finalización de la Relación Laboral	8.3.1	Responsabilidades en la desvinculación	28/01/2015	01/02/2015	Programado
		8.3.2	Devolución de activos.			
		8.3.3	Remoción de los derechos de acceso.			
3. SEGURIDAD CON TERCEROS	Consideraciones de Seguridad con partes externas	6.2.1	Identificación de riesgos relacionados con partes externas	04/02/2015	08/02/2015	Programado
		6.2.2	Tener en cuenta la seguridad cuando se trata con clientes			
		6.2.3	Tratamiento de seguridad en los acuerdos de terceras partes			
4. SEGURIDAD DEL ENTORNO	Seguridad Física y Ambiental	9.1.1	Perímetro de la Seguridad Física	11/02/2015	15/02/2015	Programado
		9.1.2	Controles de acceso físico			
	Trabajo seguro en Oficinas	9.1.3	Seguridad de oficinas, despachos e instalaciones	18/02/2015	22/02/2015	Programado
		9.1.5	Trabajo en Areas Seguras			
5. SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN	Clasificación y Manejo Seguro de la Información	7.1.1	Inventario de activos.	25/02/2015	01/03/2015	Programado
		7.1.2	Propiedad de los activos.			
		7.2.1	Guías de clasificación.			
	Análisis de Riesgos y Plan de Tratamiento	6.2.1	Identificación de riesgos relacionados con partes externas	03/03/2015	08/03/2015	Programado
	Uso Aceptable de los recursos de Información	7.1.3	Uso adecuado de los activos.	11/03/2015	15/03/2015	Programado
		7.2.2	Etiquetado y manejo de la información			
		10.7.3	Procedimiento en el manejo de la información			
		11.3.2	Equipo desatendido			

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO	FECHA DE INICIO	FECHA DE FIN	ESTADO
		11.3.3	Política de escritorio y pantalla limpios			
		10.1.1	Procedimientos de operación documentados			
		10.7.4	Seguridad de la documentación de sistemas			
		10.8.5	Sistemas de información del negocio			
		15.1.3	Protección de los registros de la organización.			
		15.1.4	Proteccion de datos y de la privacidad de la información de las personas			
		15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información.			
	Uso Aceptable de los recursos de Información	7.1.3	Uso adecuado de los activos.	18/03/2015	22/03/2015	Programado
		11.3.2	Equipo de usuario desatendido			
		11.3.3	Política de escritorio y pantalla limpios			
		15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información.			
	Intercambio de Información.	9.2.7	Retiro de bienes	25/03/2015	29/03/2015	Programado
	Seguridad en la Entrega, Retiro y Carga de Documentos.	10.8.3	Medios físicos en tránsito	01/04/2015	05/04/2015	Programado
	Seguridad en el Re Uso o Eliminación de Equipos Informáticos y Medios de Almacenamiento	10.7.2	Eliminación de los medios	05/12/2014	10/12/2014	Programado
		9.2.6	Seguridad en la reutilización o eliminación de los equipos			
	Procedimiento de Instalación	9.2.1	Ubicación y protección de los equipos	08/04/2014	12/04/2014	Programado

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO	FECHA DE INICIO	FECHA DE FIN	ESTADO
	de Equipos	6.1.4	Proceso de autorización para las instalaciones de procesamiento de la información			
		15.1.2	Derechos de propiedad intelectual (DPI)			
	Mantenimiento preventivo y Correctivo	9.2.4	Mantenimiento de los equipos	15/04/2015	19/04/2015	Programado
		10.10.5	Registro de fallas			
	Retiro de Activos de Información (Equipos de Computo)	9.2.7	Retiro de bienes	22/04/2015	26/04/2015	Programado
		10.8.3	Medios físicos en tránsito			
6: GESTIÓN DE OPERACIONES DE SISTEMAS	Acuerdo de Uso de Dispositivos removibles y Cámaras digitales	10.7.1	Gestión de los medios removibles	29/04/2015	03/05/2015	Programado
	Respaldo y Restauración de la Información.	10.5.1	Respaldo (back-up) de la información	06/05/2015	10/05/2015	Programado
	Uso Aceptable de los recursos de Información	10.3.2	Aceptación de sistemas	13/05/2015	17/05/2015	Programado
		10.10.1	Registro de Auditoría			
		10.10.2	Monitoreo del uso del sistema			
		10.10.3	Protección de la información del registro			
		10.10.4	Registro de administradores y operadores			
		10.10.6	Sincronizaqción de relojes			
		12.6.1	Control de las vulnerabilidades			
		13.1.1	Reporte de eventos de la seguridad de información.			
		15.3.1	Control de auditoria de los sistemas de información			

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO	FECHA DE INICIO	FECHA DE FIN	ESTADO
		15.3.2	Proteccion de las herramientas de auditoria de los sistemas de información			
	Control de Cambios en los Sistemas y recursos de TI	10.1.2	Gestión de cambios	20/05/2015	24/05/2015	Programado
	Intercambio de información	10.8.1	Politicas y procedimiento de intercambio de información	27/05/2015	31/05/2015	Programado
		10.8.2	Acuerdos de intercambio			
7. CONTROL DE ACCESOS	Administración de los Derechos de Acceso de los Usuarios	11.1.1	Política de control de acceso	03/06/2015	07/06/2015	Programado
		11.2.1	Registro de usuarios			
		11.2.2	Gestión de privilegios			
		11.2.4	Revisión de los derechos de acceso de los usuarios			
	Uso de contraseñas	11.3.1	Uso de contraseñas	10/06/2015	14/06/2015	Programado
		11.2.3	Gestión de contraseñas de usuario			
		11.5.3	Sistema de gestion de contraseñas			
	Administración de los Derechos de Acceso de Usuarios.	11.4.1	Políticas sobre el uso de servicios en red	17/06/2015	21/06/2015	Programado
		11.4.3	Identificación de redes en la red			
		11.4.4	Protección del diagnostico remoto y de la configuración de puerto			
		11.4.5	Segregación en redes			
		11.4.6	Control de conexión de red			
		11.4.7	Control de direccionamiento de la red			
	Uso Aceptable de los Recursos	11.5.1	Procedimiento de conexión segura	24/06/2015	28/06/2015	Programado

Grupo Procedimientos	Nombre Procedimiento	C	CONTROL ISO	FECHA DE INICIO	FECHA DE FIN	ESTADO
	Informáticos	11.5.2	Identificación y autenticación de usuario			
		11.5.4	Uso de utilitarios (utilities) del sistema			
		11.5.5	Sesión inactiva			
		11.5.6	Limitacion del tiempo de conexión			
8. GESTION DE INCIDENTES Y CONTINUIDAD DE NEGOCIO	Gestión de Incidentes en Seguridad de la Información	13.2.1	Responsabilidades y procedimientos.	01/07/2015	05/07/2017	Programado
		13.2.3	Recolección de evidencia			
		6.1.6	Contacto con autoridades			

Anexo 02

Cronograma de la Implementación – Resultado del Analisis de Riesgos

N°	Activo	Riesgo	Opciones de tratamiento	N° Control	Nombre del Control ISO 27001	Área Responsable	Inversión Económica	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Riesgo Residual	Estado
1	Switch	4	Transferir	**TRANSFERIDO**						28/12/2014		Programado
		4	Reducir	10.10.2	Uso del sistema de monitoreo	JEFE SGSI	NO	17/12/2014	21/12/2014	28/12/2014	2	Programado
2	Patch Panel	4	Transferir	**TRANSFERIDO**						28/12/2014		Programado
3	Formato de préstamo de equipo	4	Reducir	10.7.3	Procedimientos para el manejo de información	JEFE SGSI	NO	11/03/2015	15/03/2015	20/03/2015	2	Programado
4	Orden de salida de equipos	4	Reducir	10.7.3	Procedimientos para el manejo de información	JEFE SGSI	NO	11/03/2015	15/03/2015	20/03/2015	2	Programado
5	Jefe de Unidad de Gestión de Informática	4	Reducir	8.1.1	Roles y responsabilidades	ADMINISTRACION	NO	07/01/2015	11/01/2015	17/01/2015	2	Programado
6	Encargado de Help Desk	4	Reducir	8.1.1	Roles y responsabilidades	ADMINISTRACION	NO	07/01/2015	11/01/2015	17/01/2015	2	Programado
7	Antivirus Coorporativo NOD32	4	Reducir	13.1.1	Reporte de eventos en la seguridad de la información	JEFE SGSI	NO	13/05/2015	17/05/2015	22/05/2015	2	Programado
8	Microsoft Excell	**RIESGO ACEPTABLE**										

Anexo N° 7: Clases de amenazas

TIPO	AMENAZA	CÓDIGO	Descripción
ERROR Y FALLOS NO INTENCIONADOS	Alteración de la información	AEF01	Alteración accidental de la información.
	Caída de aplicaciones o del sistema operativo	AEF02	
	Caída de servicios del proveedor	AEF03	
	Caída del sistema por agotamiento de recursos	AEF04	La carencia de recursos suficientes provoca caída del sistema cuando la carga de trabajo es desmesurada
	Deficiencias en la organización	AEF05	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión
	Degradación de la información	AEF06	Degradación accidental de la información
	Destrucción de información	AEF07	Pérdida accidental de información
	Difusión de software dañino (Virús, spyware, etc)	AEF08	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
	Divulgación de información	AEF09	Revelación por indiscreción
	Errores de configuración	AEF10	Introducción de datos de configuración erróneos
	Errores de los usuarios	AEF11	Equivocaciones de las personas cuando usan los servicios, datos, etc.
	Errores de mantenimiento / actualización de equipos (hardware)	AEF12	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. Equipos: UPS, servidores, PCs, Grupos electrógenos, etc
	Errores de mantenimiento / actualización de programas (software)	AEF13	Defectos en los procedimientos o controles de actualización del código que permitan que sigan utilizándose programas con defectos conocidos y reparados por el fabricante
	Errores de monitorización (log)	AEF14	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos
	Errores de re-enrutamiento	AEF15	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
	Errores de secuencia	AEF16	Alteración accidental del orden de los mensajes transmitidos
	Errores del administrador	AEF17	Equivocaciones de personas con responsabilidad de instalación y operación
	Escapes de información	AEF18	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en si misma se vea alterada
	Indisponibilidad del personal / Ausencia accidental	AEF19	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bactriológica
	Introducción de información incorrecta	AEF20	Inserción accidental de información incorrecta

TIPO	AMENAZA	CÓDIGO	Descripción
	Pérdida de personal	AEF21	fallecimiento, enfermedad terminal
	Problemas de transporte	AEF22	
	Vulnerabilidad de los programas (software)	AEF23	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar
ATAQUES INTENCIONADOS	Abuso de privilegios de acceso	AAI01	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas
	Acceso no autorizado	AAI02	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización
	Alteración de secuencia	AAI03	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados
	Análisis de tráfico	AAI04	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir de análisis del origen, destino, volumen y frecuencia de los intercambios. También se denomina "Monitorización del tráfico".
	Ataque destructivo (Vandalismo, terrorismo, etc)	AAI05	Vandalismo, terrorismo, acción militar. Motín, protesta, bombas, violencia laboral Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas en forma temporal.
	Caída de aplicaciones o del sistema operativo	AAI06	
	Caída de servicios del proveedor	AAI07	
	Corrupción de la información	AAI08	Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio
	Denegación de servicio	AAI09	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada
	Desciframiento y/o robo de contraseña	AAI10	
	Destrucción de la información	AAI11	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio
	Difusión de software dañino (Virús, spyware, etc)	AAI12	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
	Divulgación de información	AAI13	Revelación de información
	Extorsión	AAI14	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido
	Fraudes	AAI15	

TIPO	AMENAZA	CÓDIGO	Descripción
	Indisponibilidad del personal (Huelgas, absentismo laboral)	AAI16	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.
	Ingeniería social	AAI17	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero
	Intercepción de información (alámbrica o inalámbrica)	AAI18	El atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada
	Introducción de falsa información	AAI19	Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio
	Intrusión física	AAI20	
	Manipulación de hardware y/o equipos	AAI21	
	Manipulación de la configuración	AAI22	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujo de actividades, registro de actividad, encaminamiento, etc.
	Manipulación de programas	AAI23	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona no autorizada la utiliza
	Modificación de la información	AAI24	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio
	Ocupación enemiga	AAI25	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo
	Pérdida de personal / Renuncia	AAI26	Renuncia
	Re-enrutamiento de mensajes	AAI27	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
	Repudio	AAI28	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: Negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: Negación de haber recibido un mensaje o comunicación. Repudio de entrega: Negación de haber recibido un mensaje para su entrega a otro.
	Robo de equipos	AAI29	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los mas habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
	Robo de información	AAI30	
	Sabotaje	AAI31	

TIPO	AMENAZA	CÓDIGO	Descripción
	Simulación de IP	AAI32	
	Suplantación de la identidad del usuario	AAI33	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de éste para sus fines propios
	Uso no previsto	AAI34	Utilización de los recursos para fines no previstos, tipicamente de interés personal: juegos, consultas personales en internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
INFLUENCIA SOCIAL ECONÓMICO	Caída general del servicio eléctrico	ASE01	Caída general en la zona o región
	Caída general del servicio telefónico	ASE02	Caída general en la zona o región
	Crisis financiera	ASE03	
	Epidemias	ASE04	
DESASTRES NATURALES	Daños por agua / Inundación	ADN01	Inundaciones: Posibilidad de que el agua acabe con recursos del sistema
	Deslizamientos / Huaycos	ADN02	
	Fuego / Incendio	ADN03	Incendio: Posibilidad de que el fuego acabe con recursos del sistema
	Huracanes	ADN04	
	Incendios forestales	ADN05	
	Inundaciones	ADN06	
	Terremotos	ADN07	
	Tormentas	ADN08	
	Tornados	ADN09	
	Tsunamis o maremotos	ADN10	
DE ORIGEN INDUSTRIAL	Avería de origen fisico o lógico	AOI01	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema
	Condiciones inadecuadas de temperatura y/o humedad	AOI02	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad
	Contaminación electromagnética	AOI03	Interferencias de radio, campos magnéticos, luz ultravioleta
	Contaminación mecánica	AOI04	Vibraciones, polvo, suciedad
	Corte de suministro eléctrico	AOI05	Cese de alimentación de potencia
	Daños por agua	AOI06	Escapes, fugas, inundaciones: Posibilidad de que el agua acabe con recursos del sistema
	Degradación de los soportes de almacenamiento de la información	AOI07	Como consecuencia del paso del tiempo
	Desastres industriales	AOI08	Otros desastres debido a la actividad humana: exposiciones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico

TIPO	AMENAZA	CÓDIGO	Descripción
	Emanaciones electromagnéticas	AOI09	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque
	Explosión	AOI10	
	Falla en la línea telefónica	AOI11	Corte, pérdida del servicio telefónico
	Fallo de servicios de comunicaciones / red	AOI12	Cese de la capacidad de transmitir datos de un sitio a otro. Tipicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender el tráfico presente
	Fuego / Incendio	AOI13	Incendio: Posibilidad de que el fuego acabe con recursos del sistema
	Interrupción de otros servicios y suministros esenciales	AOI14	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner refrigerante
	Materiales peligrosos	AOI15	

Anexo N° 8: Clases de vulnerabilidades

CAPA	DESCRIPCIÓN	CÓDIGO
SEGURIDAD DE LOS RECURSOS HUMANOS	Carencia de toma de conciencia en seguridad	VRH01
	Empleados desmotivados	VRH02
	Falla de mecanismos de monitoreo	VRH03
	Falta de capacitación y educación en seguridad de información	VRH04
	Falta de personal para desempeñar el rol	VRH05
	Falta de políticas y procedimientos operativos especificos	VRH06
	Falta de procesos disciplinarios formales	VRH07
	Falta definir processo que asegure la devolución de activos	VRH08
	Falta definir responsabilidades de seguridad	VRH09
	Falta definir responsabilidades por cese o cambio del personal	VRH10
	Funciones y responsabilidades de seguridad de información no definidas	VRH11
	Inadecuada verificación de antecedentes	VRH12
	Incumplimiento de las políticas para el uso correcto de las telecomunicaciones	VRH13
	No eliminar los accesos por cese o descanso temporal	VRH14
	Términos y condiciones de contratación no incluyen aspectos de seguridad de información	VRH15
CONTROL DE ACCESOS	Carencia del uso de claves seguras	VCA01
	Carencia o Inadecuada revisión de los derechos de acceso del usuario	VCA02
	Deficiencia en la identificación y autenticación del usuario	VCA03
	Falla en la protección del puerto de diagnóstico y configuración remoto	VCA04
	Falla en la restricción y control de privilegios	VCA05
	Falta de cierre de sesión por inactividad	VCA06
	Falta de control estricto en el uso de las utilidades del sistema	VCA07
	Falta de controles en la asignación de claves secretas a usuarios	VCA08
	Falta de identificación automática del equipo en la red	VCA09
	Falta de limitación del tiempo de conexión en las aplicaciones de alto riesgo	VCA10
	Falta de políticas y procedimientos para teletrabajo	VCA11
	Falta de procedimientos para el registro y des-registro de usuarios	VCA12
	Falta de protección del equipo de comunicación móvil	VCA13
	Falta de restricción del acceso a la información para usuarios y personal de soporte	VCA14
	Falta o falla del control de routing de la red	VCA15
	Falta o inadecuado aislamiento de los sistemas sensibles	VCA16
	Inadecuada segregación de redes	VCA17
	Inadecuado control de conexión a la red	VCA18
	Inadecuado sistemas de gestión de claves secretas (no interactivos, claves inseguras)	VCA19
	Inadecuados métodos de autenticación del usuario para conexiones externas	VCA20
	Incumplimiento de la política de escritorios limpios	VCA21
	Incumplimiento de las políticas de control de accesos	VCA22
	Incumplimiento de las políticas sobre el uso de los servicios de red	VCA23
	Incumplimiento en la protección de equipos por parte de usuarios	VCA24
	Procedimiento inseguro para el registro	VCA25
SEGURIDAD FISICA Y AMBIENTAL	Almacenes desprotegidos	VFA01
	Areas inseguras	VFA02
	Carencia de controles de seguridad física perimetral	VFA03
	Carencia de programas para sustituir equipos	VFA04
	Control inadecuado en áreas de acceso público, entrega y carga	VFA05
	Falla en la seguridad de la eliminación o re-uso del equipo	VFA06
	Falla en la seguridad física de oficinas, habitaciones y medios	VFA07

CAPA	DESCRIPCIÓN	CÓDIGO
	Falta de control en el traslado de equipos, información o software fuera de la empresa	VFA08
	Falta de instalaciones del sistema electrico	VFA09
	Falta o deficiencia en protección contra amenazas externas y ambientales	VFA10
	Inadecuadas medidas de control de seguridad para equipos fuera del local	VFA11
	Inadecuado mantenimiento de equipos	VFA12
	incumplimiento de controles en telecomunicaciones	VFA13
	Incumplimiento de controles seguridad física perimetral	VFA14
	Incumplimiento de políticas y procedimientos de seguridad física y ambiental	VFA15
	Mal cuidado de equipos	VFA16
	Mala ubicación y protección de equipos	VFA17
	Susceptibilidad de equipos a variaciones de voltaje	VFA18
	Ubicación en áreas sujeta a inundaciones	VFA19
GESTION DE OPERACIONES Y COMUNICACIONES	Carencia de backup o respaldo de la información	VOC01
	Complicadas interfaces para usuarios	VOC02
	Diagramas o esquemas no formalizados de la red	VOC03
	Falla en la sincronización de relojes	VOC04
	Fallas en la protección de la documentación del sistema	VOC05
	Falta de acuerdos de intercambio	VOC06
	Falta de implementación de procedimientos de control de cambios	VOC07
	Falta de procedimientos para el manejo de la información	VOC08
	Falta de procedimientos para el monitoreo de los sistemas	VOC09
	Falta de procedimientos para la gestión de los medios removibles	VOC10
	Falta de protección de la información públicamente disponible	VOC11
	Falta de protección en el comercio electrónico	VOC12
	Falta de protección en las transacciones en línea	VOC13
	Falta de protección en redes públicas de conexión	VOC14
	Falta de protección para los medios físicos en tránsito	VOC15
	Falta de registro de fallas e incidencias	VOC16
	Falta de registros de auditoría	VOC17
	Falta de registros del administrador y operador del sistema	VOC18
	Falta de seguridad de los servicios de la red	VOC19
	Falta de separación de los ambientes de desarrollo, testing y producción	VOC20
	Falta documentar y difundir procedimientos de operación	VOC21
	Falta especificación del requerimientos	VOC22
	Falta o falla de controles contra código malicioso	VOC23
	Falta o falla de controles contra código móvil	VOC24
	Falta o Inadecuada segregación de funciones	VOC25
	Inadecuada eliminación de los medios	VOC26
	Inadecuada entrega de servicios por parte de terceros	VOC27
	Inadecuada gestión de cambios	VOC28
	Inadecuada gestión de la capacidad y uso de recursos	VOC29
	Inadecuada gestión y control de la red	VOC30
	Inadecuada protección de mensajes electrónicos	VOC31
	Inadecuada protección del registro de la información	VOC32
	Inadecuado manejo de cambios en los servicios de terceros	VOC33
	Inadecuado monitoreo y revisión de los servicios de terceros	VOC34
	Inadecuados criterios de aceptación de los sistemas	VOC35
	incumplimiento de las políticas para la protección de los sistemas de información	VOC36
	Incumplimiento de las políticas y procedimientos de intercambio de información	VOC37

CAPA	DESCRIPCIÓN	CÓDIGO
MANTENIMIENTO, DESARROLLO Y ADQUISICIÓN DE SISTEMAS	Carencia de validación de datos procesados	VDA01
	Deficiencia en el estudio de licenciamiento de software	VDA02
	Entregables no definidos	VDA03
	Falla en la protección de la integridad del mensaje en las aplicaciones	VDA04
	Falta de chequeos de validación en las aplicaciones	VDA05
	Falta de control de acceso al código fuente del programa	VDA06
	Falta de control de Licencias de software	VDA07
	Falta de inclusión de controles de seguridad en los requerimientos del negocio	VDA08
	Falta de manuales técnicos y operativos del software	VDA09
	Falta de política de restricciones sobre los cambios en los paquetes de software	VDA10
	Falta de procedimiento para controlar la instalación de software	VDA11
	Falta de procedimientos de control de cambios	VDA12
	Falta de pruebas	VDA13
	Falta de revisiones técnicas de las aplicaciones después de cambios en el sistema operativo	VDA14
	Falta de seguimiento de los contratos con terceros	VDA15
	Falta de supervisión en el desarrollo de software proporcionado por terceros	VDA16
	Falta de validación de la data de entrada para las aplicaciones	VDA17
	Falta de validación de la data de salida para las aplicaciones	VDA18
	Falta, deficiencia o incumplimiento de políticas sobre el uso de controles criptográficos	VDA19
	Filtración de información	VDA20
	Inadecuada selección y protección de la data de prueba del sistema	VDA21
	Inadecuado control de las vulnerabilidades técnicas	VDA22
	Incumplimiento con la metodología de desarrollo de software	VDA23
	Planificación no formalizadas	VDA24
	Uso inadecuado o deficiente de las llaves y técnicas de criptografía	VDA25