UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"
ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE

"Plan de gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque"

TESIS

Presentada para optar el Grado Académico de Maestro en Ingeniería de Sistemas con mención en Gerencia de Tecnologías de la Información y Gestión del Software

AUTORA:

Ing. LLuén Montañez, Erika Zarela

ASESOR:

MSc. Fiestas Rodriguez, Pedro

LAMBAYEQUE - PERÚ

2021

"Plan de Gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque"

Ing. Erika Zarela Lluén Montañez
Autor

MSc. Pedro Fiestas Rodríguez
Asesor

Tesis presentada a la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el Grado Académico de: MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DE SOFTWARE

Aprobado por:

Dr. Ernesto Karlo Celi Arevalo
Presidente del jurado

Dr. Santos Henry Guevara Quilichi
Secretario del jurado

Mg. Jesús Bernardo Olavarría Paz
Vocal del jurado

Lambayeque, 2021

ACTA DE SUSTENTACIÓN VIRTUAL DE TESIS

Siendo las 05:00 p.m. del día martes 09 de febrero de 2021, se dio inicio a la Sustentación Virtual de Tesis soportado por el sistema Blackboard Ultra, preparado y controlado por la Unidad de Tele Educación de la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque, con la participación en la Video Conferencia de los miembros del Jurado, nombrados con Resolución N°1435-2019-EPG, de fecha 18 de octubre de 2019, conformado por:

Dr. ERNESTO KARLO CELI AREVALO	PRESIDENTE
Dr. SANTOS HENRY GUEVARA QUILICHE	SECRETARIO
Mg. JESUS BERNARDO OLAVARRIA PAZ	VOCAL
Mg. SEGUNDO PEDRO FIESTAS RODRIGUEZ	ASESOR

Para evaluar el informe de tesis de la tesista ERIKA ZARELA LLUEN MONTAÑEZ, candidata a optar el grado de MAESTRA EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE con la tesis titulada "PLAN DE GESTION DE LA CONTINUIDAD DE NEGOCIO BASADO EN LA NORMA ISO 22301 PARA LA OFICINA DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO REGIONAL DE LAMBAYEQUE".

El Sr. Presidente, después de transmitir el saludo a todos los participantes en la Video Conferencia de la Sustentación Virtual ordenó la lectura de la Resolución Nº057-2021-EPG de fecha 01 de febrero de 2021 que autoriza la Sustentación Virtual del Informe de Tesis correspondiente, luego de lo cual autorizó a la candidata a efectuar la Sustentación Virtual, otorgándole 25 minutos de tiempo y autorizando también compartir su pantalla.

Culminada la exposición de la candidata, se procedió a la intervención de los miembros del jurado, exponiendo sus opiniones y observaciones correspondientes, posteriormente se realizaron las preguntas al candidato.

Culminadas las preguntas y respuestas, el Sr. Presidente, autorizó el pase de los miembros del Jurado a la sala de video conferencia reservada para el debate sobre la Sustentación Virtual del Informe de tesis realizada por la candidata, evaluando en base a la rúbrica de sustentación y determinando el resultado total de la tesis con 17 puntos, equivalente a Bueno, quedando la candidata

apta para optar el Grado de MAESTRA

EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE.

Se retornó a la Video Conferencia de Sustentación Virtual, se dio a conocer el resultado, dando lectura del acta y se culminó con los actos finales en la Video Conferencia de Sustentación Virtual.

Siendo las 06:05 pm se dio por concluido el acto de Sustentación Virtual.

PRESIDENTE

Dr. Santos Henry Guevara Quiliche

SECRETARIO

Mag. Jesús Bernardo Olavarria Paz

VOCAL

ASESOR

Declaración Jurada de Originalidad

Yo, **Ing. Erika Zarela Lluén Montañez,** investigador principal, y **MSc. Pedro Fiestas Rodríguez,** asesor del trabajo de investigación "Plan de Gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque", declaramos bajo juramento que este trabajo no ha sido plagiado, ni contiene datos falsos. En caso se demostrará lo contrario, asumo responsablemente la anulación de este informe y por ende el proceso administrativo a que hubiere lugar. Que puede conducir a la anulación del título o grado emitido como consecuencia de este informe.

Lambayeque, Marzo del 2021

Nombre del autor : Ing. Erika Zarela Lluén Montañez.

Nombre del asesor : MSc. Pedro Fiestas Rodríguez.

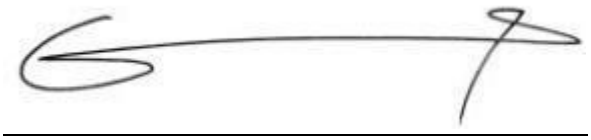
CONSTANCIA DE APROBACION DE ORIGINALIDAD DE TESIS

Yo, **MSc. Segundo Pedro Fiestas Rodríguez**, Asesor de Tesis, del estudiante **Ing. Erika Zarela Lluén Montañez**

Titulada:
"Plan de gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque", luego de la revisión exhaustiva del documento constato que la misma tiene un indice de similitud de 14% verificable en el reporte de similitud del programa Turnitin.

El suscrito analizó dicho reporte y concluyyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo

Lambayeque, 20 de Noviembre de 2023



Ms. Pedro Segundo Fiestas Rodriguez
Asesor

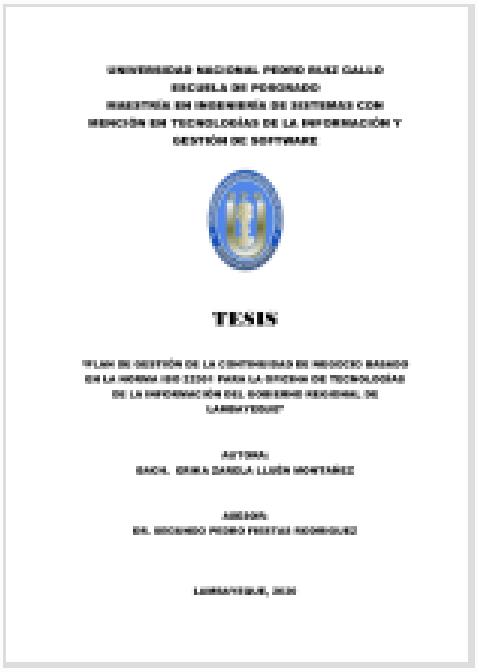
turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Erika Zarela Lluen Montañez
Título del ejercicio:	Informe final de tesis de maestria
Título de la entrega:	Informe final de tesis de maestria
Nombre del archivo:	Informe_final_de_tesis.docx
Tamaño del archivo:	829.39K
Total páginas:	169
Total de palabras:	46,575
Total de caracteres:	253,814
Fecha de entrega:	06-sep-2020 11:03a.m. (UTC-0500)
Identificador de la entrega:	1380678368



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
ESCUELA DE POSGRADO
MAESTRIA EN INGENIERIA DE SISTEMAS CON
MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y
GESTIÓN DE SOFTWARE

TESIS

"PLAN DE GESTIÓN DE LA CONTINUIDAD DE NEGOCIO BASADO
EN LA NORMA ISO 22301 PARA LA OFICINA DE TECNOLOGÍAS
DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE
LAMBAYEQUE"

AUTORA:
BACH. ERIKA DANILA LLUEN MONTAÑEZ

ASESOR:
DR. SEGUNDO PEDRO FIESTAS RODRIGUEZ

LAMBAYEQUE, 2020

MSc. Pedro Fiestas Rodriguez - Asesor

Informe final de tesis de maestría

INFORME DE ORIGINALIDAD

14%	14%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unprg.edu.pe Fuente de Internet	1%
2	hdl.handle.net Fuente de Internet	1%
3	intranet1.sbs.gob.pe Fuente de Internet	1%
4	www.vprog.it Fuente de Internet	1%
5	tesis.usat.edu.pe Fuente de Internet	<1%
6	repositorio.ucv.edu.pe Fuente de Internet	<1%
7	www.piuraheraldo.net Fuente de Internet	<1%
8	repositorio.utn.edu.ec Fuente de Internet	<1%
9	www.sectorturismo.gob.mx Fuente de Internet	<1%

MSc. Pedro Fiestas Rodriguez - Asesor

DEDICATORIA

Dedico esta Tesis principalmente a Dios, por permitirme lograr un avance más en mi vida profesional. A mi esposo e hijos, por estar siempre a mi lado apoyándome y brindándome su apoyo y ánimos para poder lograr este objetivo.

AGRADECIMIENTO

Agradezco a mi familia por su apoyo incondicional y a mi asesor por brindarme sus conocimientos y su apoyo constante, y permitir de esa forma desarrollar esta investigación brindando un aporte para otras investigaciones futuras.

INDICE

INDICE DE TABLAS

INDICE DE GRÁFICOS

RESUMEN

El presente estudio aborda uno de los problemas más importantes de una institución que gestiona sus procesos a través del uso de tecnologías de la información y las comunicaciones. Esta dependencia de las TIC hace que cualquier incidente que afecte el funcionamiento de algún recurso informático puede conllevar a un impacto negativo significativo en la institución. El Gobierno Regional de Lambayeque (GRL), no es ajeno a este problema, pues casi la totalidad de sus procesos son gestionados a través de aplicaciones informáticas que han sido desarrollados o adecuados en su Oficina de Tecnologías de la Información (OFTI); además de contar con un soporte tecnológico informático considerable.

Una de las estrategias más usadas para la gestión preventiva y correctiva de los incidentes relacionados con las tecnologías de la información es la gestión de la continuidad del negocio (para este estudio, se considera como continuidad de los procesos). Por ello, el marco de referencia tomado como guía fue la ISO/IEC 22301 para desarrollar, mediante métodos descriptivos, cada una de las fases y buenas prácticas que la norma determina. Los datos fueron obtenidos de la misma entidad.

Los resultados de la investigación fueron validados a través de un procedimiento no experimental, el cual recoge las percepciones de los principales responsables y con autoridad, de los procesos institucionales y de la gestión de las tecnologías de la información en el GRL. El método aplicado fue Delphi.

Palabras clave: proceso crítico, análisis de impacto en el negocio, análisis de riesgos, plan de continuidad, ISO/IEC 22301

ABSTRACT

INTRODUCCIÓN

El avance y la fácil disponibilidad de tecnologías nuevas y útiles hoy han permitido a miles de empresas en todo el mundo, poner en práctica y convertirse en dependientes en gran medida de la tecnología para sus necesidades de negocio. Las tecnologías de la información (TI) ha invadido y ha demostrado sus enormes beneficios incluso en la más pequeña de las organizaciones. Hoy en día no es posible lograr eficiencia operativa en cualquier empresa, grande o pequeña, sin el uso de alguna tecnología informática o de telecomunicaciones relacionadas (Thejendra, 2014).

El uso de TI en una empresa se ve enmarcada mediante el concepto de Gobierno de TI, el cual integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa, soporta los objetivos del negocio y facilita el aprovechamiento al máximo de su información, maximiza los beneficios, capitaliza las oportunidades y permite ganar ventajas competitivas (Ramírez, Calderas, & Benavides, 2012).

Con el entorno y dinámicas competitivas de la actualidad, contar con tecnología de información y comunicaciones no supone por sí misma una ventaja competitiva para las organizaciones. Es la gestión de esa tecnología la que puede dar una ventaja o marcar factor diferencial para el éxito de éstas. De acuerdo a esto, apropiarse de un modelo de gobierno IT, para esta gestión, es un elemento clave para el cumplimiento de los objetivos de la empresa (Marulanda Echevarría, López Trujillo, & Cuestas Iglesias, 2009).

La incorporación del Gobierno de TI y una adecuada Gestión de TI en las empresas, permiten lograr muchos beneficios, generando mayor valor a las empresas. Uno de los componentes del Gobierno de las TI es la Gestión de la Continuidad del negocio y de los procesos.

En el Gobierno Regional de Lambayeque (GRL) la política informática de las últimas gestiones ha permitido la priorización del componente “tecnología” como un aspecto clave para el logro de los objetivos estratégicos de la Sede del Gobierno Regional Lambayeque en los próximos años, los cuales se orientan hacia una excelencia en el servicio al ciudadano fortaleciendo la transparencia y acceso a la información como imagen de una buena gestión institucional. Los servicios que brinda el Gobierno Regional deben ser “efectivos, eficientes y oportunos”. Al incorporar tecnología en la ejecución de los procesos y procedimientos administrativos de esta Institución se debe realizar con base a una planificación que tenga una visión clara y objetivos concretos y realistas, en función al

presupuesto que se tiene, y deben ser alineados a los objetivos institucionales con un enfoque de soporte a dichos procesos.
La Gestión de la Continuidad de los procesos busca establecer las acciones a implementarse frente a los riesgos a los que están expuestos el personal y bienes en general ubicados en la Sede del GRL, motivo por el cual se garantice el restablecimiento, operatividad y funcionamiento de los servicios en el menor tiempo posible.

Un Sistema de Continuidad de los procesos implica un análisis de los posibles riesgos informáticos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que se ha analizado los riesgos más frecuentes, y como reducir su posibilidad de ocurrencia, así como las acciones a seguir en caso se presente la contingencia, resultando necesario que este sistema incluya la recuperación de desastres y conocer cómo se restaura la continuidad del servicio informático en forma rápida, con el menor costo y perdidas posibles.

En ese sentido, el GRL a través de la Oficina de Tecnologías de la Información - OFTI, necesita de un **Plan de Gestión de la continuidad de negocio** el mismo que define el enfoque tecnológico a seguir en los próximos seis (06) años, es decir del periodo 2020 al 2026; y la forma como este enfoque se aplica en los procesos; y la manera como se implanta en la Sede del GRL.

Objetivo general

Elaborar un Plan de Gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque

Objetivos específicos

a. Analizar los procesos institucionales con la finalidad de determinar su criticidad e identificar los roles, funciones y soporte tecnológico crítico que será considerado en el Plan de gestión de la continuidad; así como sus periodos de recuperación y tiempos máximo aceptables de caída,
b. Analizar el impacto de la caída de los procesos críticos a través de una ponderación de su criticidad en los siguientes factores: financiero, afectación a usuarios internos, afectación a usuarios externos, afectación de la infraestructura, afectación a aspectos legales/contractuales.
c. Realizar una evaluación de los riesgos de cada activo tecnológico considerado como crítico con la finalidad de determinar los niveles de exposición al riesgo e identificar los escenarios de riesgo.
d. Definir como estrategia de contingencia las acciones preventivas y correctivas para cada escenario de riesgo.

e. Validar el modelo de gestión de continuidad de los procesos propuesto, a través del método Delphi.

I. DISEÑO TEÓRICO

1.1. Antecedentes de la investigación

De la revisión de trabajos de investigación similares, se describe a continuación los antecedentes de la investigación encontrados, los que se tomarán en cuenta en el desarrollo del Modelo de gestión de una mesa de ayuda al usuario de TI propuesto.

Ordóñez (2017), en su tesis titulada: "Elaboración de un plan de contingencia para el departamento de soporte técnico de la Facultad de ingeniería en electricidad y computación para garantizar la continuidad de sus actividades ante desastres informáticos", en su trabajo se realizó un análisis de riesgos y se elaboró un plan de contingencia para que el equipo técnico pueda prever y actuar ante eventos catastróficos que impidan el desarrollo continuo de su funcionamiento. Con este estudio llegó a la conclusión de que la infraestructura de tecnología debe tener un funcionamiento continuo, ante cualquier inconveniente o contingencia, ya que esta área siempre debe estar disponible para los usuarios que dependen de esta área.
Esta investigación tiene relación con nuestro proyecto ya que buscamos analizar los riesgos y prever que los procesos paren en el área de Tecnología del gobierno Regional, sino más bien que se lleven con normalidad.

González (2015), en su tesis titulada: "Elaboración de un plan de auditoría para avaluación de cumplimiento en sistemas para gestión de la continuidad del negocio basado en la normativa ISO 22301", elaboró una guía que brindó capacidades que permiten sobrevivir a situaciones complejas que amenazan la supervivencia, teniendo en cuenta los procesos críticos para el negocio. Con este estudio modeló sistemas de continuidad de negocio basado en un BIA (Bussiness Impact Analysis), que permitió identificar procesos críticos para el negoció, así como identificar las dependencias necesarias que ayudaron a continuar brindando servicios, quedando comprobado que estas herramientas automatizadas por la ISO 22301 facilita de manera óptima la toma de decisiones a equipos de auditoría.
Este trabajo tiene relación con nuestra investigación, porque se busca proponer un modelo basado en la ISO 22301 que permita gestionar documentación crítica para el gobierno Regional.

Soto y Céspedes (2019), en su tesis titulada: “Modelo de un sistema de gestión de continuidad del negocio para microfinanciera basado en la ISO/IEC 22301 y en la circular G-139-2009 de la SBS”, esta tesis implementó un modelo de gestión de la continuidad del negocio para empresas financieras, como cajas municipales, cooperativas de ahorro, crédito financieras y Edpymes. Se enfocaron en los lineamientos de la ISO/IEC 22301 para los eventos que afecten al continuo funcionamiento de procesos. Con este estudio llegaron a la conclusión de que con este modelo se mejoró la gestión de continuidad del negocio bajo la normativa ISO 22301, tomando como base el ciclo PDCA (Plan – Do – Check – Act).
Este trabajo guarda una relación estrecha con nuestro proyecto ya que buscamos implementar la norma ISO 22301 que ayude a la continuidad de negocio, este proyecto además nos ayudará a considerar y comparar el modelo que propusieron con el modelo que vamos a proponer.

Ramírez (2017) en su tesis titulada: “Modelo para la gestión de la continuidad del servicio de tecnologías de la información para empresas de tipo burocracia profesional basada en la norma técnica internacional ISO 22301”, en su investigación propuso un modelo para la gestión de continuidad de servicios de tecnologías de información que permitió que la empresas burocráticas puedan plantear estrategias tácticas para responder ante posibles incidentes o interrupciones del negocio con el fin dar continuidad a las operaciones. Llegó a la conclusión de que gracias a la estandarización de los formatos de la ISO 22301 se puede plantear un modelo de continuidad evaluando diversas pruebas en el servicio tecnológico que asegure la viabilidad de soluciones adoptadas.
Este estudio tiene relación con nuestro proyecto, porque al igual que el autor buscamos que la norma ISO 22301 fortalezca al área de Tecnología y use nuestro modelo para gestionar estrategias y medidas para que los incidentes o interrupciones no afecten a la continuidad.

Velásquez y Alva (2018) en su tesis titulada: “Modelo de gestión de riesgos de TI para contribuir en la continuidad del negocio de las microfinancieras de la región Lambayeque”, propusieron una solución que evalúa la deficiencia para gestión de riesgos de TI que puedan afectar a la continuidad de negocio en el sector microfinanciero siguiendo una serie de normativas, aplicando metodologías y estándares de gestión de riesgos. Llegaron a la conclusión de que se puede identificar procesos críticos para garantizar la continuidad del negocio en base al análisis de riesgos.

Este trabajo tiene relación con nuestra investigación ya que es un estudio realizado en nuestra región, y este estudio demuestra que proponiendo un modelo se pueden aplicar planes de acción necesarios para garantizar la continuidad del negocio, esto nos ayudará a realizar una comparativa entre su modelo y el nuestro.

1.2. Base teórica

En el desarrollo del presente trabajo de tesis, se tomó en cuenta los siguientes fundamentos teóricos:

1.2.1. Continuidad de negocio

Es el desarrollo de estrategias, planes y acciones que brindan protección o modos alternativos de operación para aquellas actividades o procesos de negocio que, de ser interrumpidos, de otra manera provocar una pérdida gravemente perjudicial o potencialmente significativa para la empresa. BCM consta de tres elementos centrales (Business Continuity Institute, 2018)

a. **La gestión de crisis y las comunicaciones** es un proceso diseñado para permitir una respuesta efectiva a un evento. Los procesos de gestión de crisis se centran en estabilizar la situación y preparar el negocio para operaciones de recuperación a través de protocolos efectivos de planificación, liderazgo y comunicación. segundo.

b. **La planificación de reanudación comercial**, o la planificación de recuperación comercial, implica la recuperación defunciones y procesos comerciales que se relacionan con la entrega de productos o servicios principales o que la respaldan a un cliente.

c. **La recuperación ante desastres de TI** aborda la recuperación de activos críticos de TI, incluidos sistemas, aplicaciones, bases de datos, almacenamiento y activos de red.

Según Martínez (2016), son procedimientos dedicados a la restauración de funciones críticas de una organización con independencia de un departamento en el que las operaciones vienen siendo realizadas. La continuidad de negocio debe tener un plan de contingencia que esté actualizado a medida que pase el tiempo, es por eso que el objetivo de este plan es subsanar deficiencias mediante evaluación continua, incluyendo el apoyo de la dirección y gestionando proyectos que cumplan con los plazos y costos establecidos.

La continuidad de negocio debe diseñarse para proporcionar respuestas inmediatas a posibles escenarios, departamentos, dependencias, instalaciones, etc. Existe un plan para cada dependencia, cabe diferenciar que no es lo mismo un plan de contingencia informático que se base en recuperación y continuidad de actividades informáticas que un plan de contingencia para un negocio el cual tenga en consideración todas las funciones que son críticas para la organización. Se debe considerar además que se debe elegir posibles amenazas dentro de un catálogo, para evaluar cuales son las más probables para que ocurran (Martinez, 2016).

1.2.2. Plan de Continuidad del Negocio

El Plan de Continuidad del Negocio abarca la identificación tanto de los procesos críticos de la organización como los recursos que utilizan. Con ello, se define una estrategia de protección que garantizará seguir brindando los productos y/o servicios en un nivel aceptable enfocándose frente a amenazas a las que se encuentra expuesta y que podrían materializarse (Spiñeira, Sheldon y Asociados, 2015).

Otro aspecto importante, para que el plan de continuidad del negocio funcione, es que la alta dirección lo considere dentro de los objetivos del negocio y que garantice su diseño, implementación, monitoreo y mejora continua para garantizar su efectividad (Spiñeira, Sheldon y Asociados, 2015).

Este plan de continuidad no solo debe enfocarse en la prevención de los incidentes, sino también en la corrección de los efectos que produzcan en caso llegaran a darse. Por ello, Espiñeira, Sheldon y Asociados, firma miembro de PricewaterhouseCoopers, menciona lo siguiente:

> *«Trabajar solamente en la prevención es incorrecto por tres (sic) razones fundamentales:*
> *1. Es imposible asegurar que se han identificados todos los posibles orígenes de contingencias (…).*
> *2. Hay riesgos que no es rentable prevenir.*
> *3. Hay riesgos que no se pueden prevenir*
> *4. Pese a que se desarrolle un excelente Plan Preventivo, las contingencias igual pueden suceder.»* (Spiñeira, Sheldon y Asociados, 2015).

Según el fragmento anterior, nos indica que no se pueden tener todos los riesgos identificados al inicio del análisis, ya que durante todo el proceso de diseño, implementación y ejecución del plan de continuidad del negocio podría aparecer más. Por un lado, no todo lo que amenaza a una empresa se puede controlar haciendo. Esto hace referencia a factores externos que una empresa no puede gestionar. Por otro lado, algunos, tal vez tengan un costo mucho menor en caso ocurrieran en comparación a tomar medidas y aplicar controles al respecto.

En términos generales, el plan de continuidad del negocio busca brindar una respuesta oportuna que permita mantener el normal funcionamiento de los procesos críticos en una empresa ante la ocurrencia de un incidente y definir un procedimiento que permita evitar que ocurra.

1.2.3. Sistema de Gestión de Continuidad del Negocio

Un sistema de gestión de continuidad del negocio (SGCN) es la parte general del sistema de gestión que se encarga de establecer, implementar, operar, monitorear, revisar y mejorar la continuidad del negocio de la organización (Ureña, 2011). Las principales ventajas que ofrece la implementación de un SGCN dentro de una empresa son las siguientes (Ferrer, 2011):

- Brindar una recuperación oportuna y eficiente de las operaciones críticas de la empresa luego de la ocurrencia de un incidente.
- Disminuir los efectos negativos causados por el caos del incidente.
- Reducir la pérdida de información de alta criticidad para el negocio.
- Eliminar la necesidad de desarrollar nuevos procesos y/o usuarios durante el periodo de recuperación.
- Reducir las decisiones que se toman durante el periodo de contingencia.

Este sistema de gestión requiere un análisis previo antes de comenzar a desarrollar los planes que lo conforman. Las principales actividades son las siguientes:

1.2.3.1. Análisis de Impacto en el Negocio

El análisis del impacto en el negocio es el proceso para analizar todas las actividades y el efecto que una interrupción podría ocasionar si llegara a materializarse (OSI, 2010). En otras palabras, es analizar e identificar los eventos que podrían afectar la continuidad de los procesos y sistemas de información críticos de la organización (Ferrer, 2011).

Para que el Análisis del Impacto en el Negocio este completo, es tener en cuenta los indicadores de tiempos estimados de recuperación (RTO) y tiempos máximo tolerables de interrupción (MTD) (SISTESEG, 2016).

1.2.3.2. Evaluación de Riesgos

La evaluación de riesgos es uno de los factores primordiales que fortalece el proceso de análisis de riesgos, es decir, en esta etapa se definen y evalúan los factores que inciden en cada uno de los procesos de negocio y de TI de la organización. Dentro de estos factores se encuentran: las personas, herramientas para el manejo de los procesos de TI, documentación de los procesos de TI, nivel de supervisión y monitoreo de los procesos, ambiente de control y controles sobre los procesos de TI; y, efecto en clientes y usuarios de TI. Durante este proceso se debe de tener en cuenta una metodología para

realizar el inventario de riesgos y la definición del universo de procesos (Alexander & AMBCI, 2012).

La evaluación de riesgos tiene una mayor visión de los potenciales eventos que impactarían en el cumplimiento de objetivos. Los eventos son analizados desde una perspectiva de probabilidad e impacto con ayuda de métodos cuantitativos y cualitativos.

Además, los riesgos se deben evaluar bajo un doble enfoque: riesgo inherente y riesgo residual (Carrillo, 2013).

Los resultados de la evaluación de riesgos deben de ser presentados en una matriz de impacto/vulnerabilidad para poder ayudar en la determinación de una respuesta y establecer métodos de tratamiento a los riesgos identificados (BSI GROUP, 2015).

1.2.4. Estrategias de Continuidad

Una estrategia de continuidad define un conjunto de acciones a realizar que emplea personas, procesos, tecnologías e infraestructura para poder responder frente a un incidente que afecte el normal funcionamiento de las operaciones de una empresa (Ureña, 2011). Las estrategias de continuidad se definen luego de realizar un análisis previo que abarca la identificación y evaluación de riesgos, y el análisis de impacto en el negocio (BIA).

Por otro lado, las estrategias definidas tienen un orden dependiendo de la importancia que tenga y la habilidad necesaria para su implementación (Alexander & AMBCI, 2012). Esto se detalla a más detalle en la imagen siguiente:

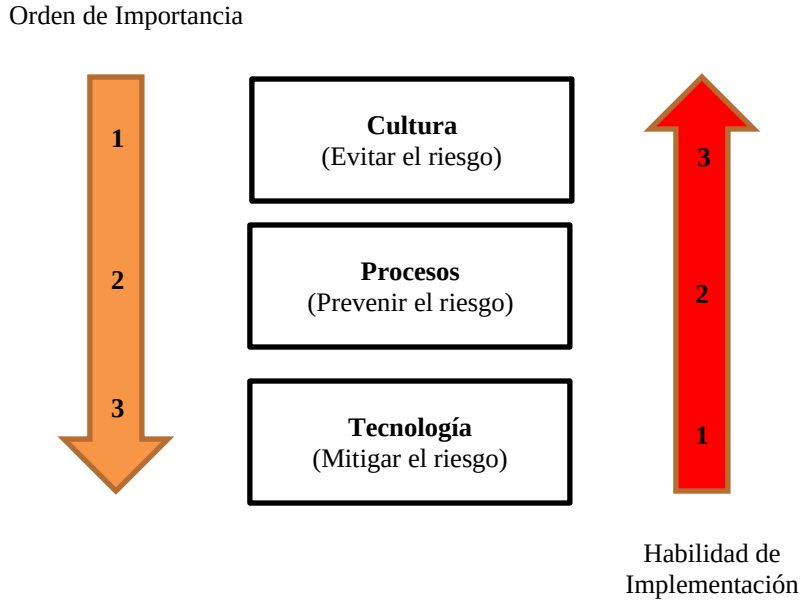


Gráfico N° 1. Orden de importancia y habilidad de implementación de las estrategias
Fuente: (Alexander & AMBCI, 2012)

Una vez realizado un análisis previo del entorno de la organización, se puede proceder a realizar los planes que contendrá el sistema de gestión de continuidad del negocio. Entre los muchos que pueden contener, los principales son los siguientes:

1.2.4.1. Plan de Recuperación de los Servicios de TI

Este plan del sistema de gestión de continuidad del negocio tiene como objetivo restaurar en el menor tiempo posible los sistemas de información que soportan los procesos críticos del negocio. Este también es conocido como plan de recuperación ante desastres y utiliza generalmente un centro físico y equipos alternos para minimizar el impacto de la caída de los servicios de TI y el costo, a nivel de ingresos, de la empresa frente a la ocurrencia de un incidente.

Como criterio de éxito principal, este plan debe ser liderado por el área de sistemas y de contar con la participación de todas las demás áreas de la empresa para poder determinar cuáles son aquellos que necesitan tener sus servicios de TI operativos lo más pronto posible.

1.2.4.2. Plan de Crisis

Este plan del sistema de gestión de continuidad del negocio tiene como objetivos principales establecer los procedimientos a seguir, definir y asignar responsabilidades,

definir los canales de comunicación oportunos y preservar la reputación de la empresa (Ferrer, 2011)

Las fases de una crisis son las siguientes:

- Identificación de señales: Realizar un análisis constante para identificar un evento de crisis
- Preparación y prevención: Realizar actividades para evitarlas y estar preparados en caso ocurriese.
- Gestión de la comunicación: Durante el periodo de crisis
- Control: Evitar que el impacto de la crisis no se extienda.
- Recuperación: Ejecución de programas para la reanudación de las actividades de la empresa.
- Aprendizaje: Realización de las lecciones aprendidas de la etapa de crisis vivida.

1.2.4.3. Plan de Entrenamiento y Capacitación

Este plan que forma parte del conjunto de planes del sistema de gestión de continuidad del negocio tiene como objetivo principal el establecimiento de un programa de capacitación y entrenamiento del personal de la empresa (González, 2015). Esto involucra también una comunicación efectiva de los objetivos del plan de continuidad del negocio para que tenga el soporte necesario y garantice el éxito de su efectividad.

Entre las principales tareas que contiene el plan de entrenamiento y capacitación se encuentran las siguientes (Ureña, 2011).

Definir los grupos a los cuales se le realizara el programa de capacitación y entrenamiento, ya que no se puede usar un mismo programa para la alta dirección que para los trabajadores del área de sistemas.

- Preparación del material del programa o estudio necesarios para el desarrollo del programa o curso de capacitación.
- La realización de los programas y dictados de cursos de capacitación.
- Definir taller o simuladores que permitan poner en prácticas los conocimientos impartidos en los programas o cursos de capacitación para evaluar la efectividad de los mismos.

1.2.4.4. Plan de Emergencias

Este plan que forma parte del conjunto de planes del sistema de gestión de continuidad del negocio tiene como objetivo principal definir los procedimientos adecuados para la preparación, control, supervisión y ejecución (Ferrer, 2011) de los ejercicios de seguridad en cada una de las sedes de la empresa con el objetivo de salvaguardar la integridad de sus colaboradores.

Esto implica definir las rutas de evacuación del lugar, los principales responsables y miembros de las brigadas, directorios con los contactos de emergencias y otros aspectos de seguridad.

Una vez terminado de definir y elaborar todos los planes del sistema de gestión de continuidad del negocio, es necesario elaborar a continuación el plan de implementación que define las etapas, tareas, recursos y tiempo que tomara realizar la implementación del sistema de gestión de continuidad del negocio dentro de la organización (Ferrer, 2011). En este se debe especificar el alcance de la implementación y el costo que implicara realizarlo.

1.2.5. Marco regulatorio / legal

1.2.5.1. NTP ISO 27001:2008

Norma Técnica Peruana de Seguridad de Información es una norma elaborada por el Comité Técnico de Normalización de codificación e Intercambio Electrónico de Datos (EDI) en el año 2008, utilizando como antecedente las ISO/IEC 27001:2005.

La NTP 27001:2008 (INDECOPI, 2008), tiene como objetivos proporcionar un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de Información como una buena práctica de la gestión de la seguridad.

Cabe mencionar que se hará mayor énfasis en lo relacionado de esta norma a la continuidad de negocios. Comprende de 11 ítems de control de seguridad que envuelven un total de 39 categorías principales, los cuales se muestran a continuación, enfatizando en el ítem de continuidad:

1. Política de seguridad
2. Seguridad Organizacional
3. Gestión de Activos

4. Seguridad en Recursos Humanos
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de accesos
8. Adquisición, desarrollo y mantenimiento de sistemas de información
9. Gestión de incidentes en la Seguridad de Información
10. **Gestión de continuidad del negocio**
11. Cumplimiento

En relación a los aspectos de la gestión de continuidad del negocio, la norma establece lo siguiente: Reaccionar ante las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los activos y asegurar la reanudación oportuna.

Este ítem en particular menciona que las formas de lograr una buena continuidad de negocio son:

a. Incluyendo la seguridad de información en la gestión de la continuidad del negocio, para ello se deben establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta efectiva ante cualquier tipo de incidente.
b. Relacionando la continuidad de negocios con la evaluación de riesgos, para ello deben ser identificadas las amenazas que pueden causar interrupciones, así como las probabilidades e impacto de dichas interrupciones.
c. Desarrollando e implementando planes de continuidad que incluyan la seguridad de información
d. Contando con un marco de planificación de la continuidad del negocio, con el fin de asegurar consistencia e identificar prioridades de prueba y mantenimiento.
e. Probando, manteniendo y reevaluando los planes de continuidad del negocio, con el fin de asegurar que estén actualizados y sean efectivos.

1.2.5.2. ISO 22301:2012 – Seguridad de la Sociedad – Sistema de Gestión de la continuidad del Negocio – Requerimientos.

Esta norma fue redactada por los principales especialistas en el tema y proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una

organización. Esta norma reemplazará al estándar BS 25999-2:2007 “Gestión de la Continuidad del Negocio: Especificaciones”. El nuevo modelo es certificable y auditable.

El estándar ISO 22301:2012 aplica el ciclo PDCA para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua de sus operaciones.

El modelo ha sido creado con consistencia con otros estándares de gestión, tales como: ISO 9001:2008, ISO 27001:2005, ISO 20000- 1:2011, ISO 14001:2004 y con el ISO 28000:2007 (Ureña, 2011).

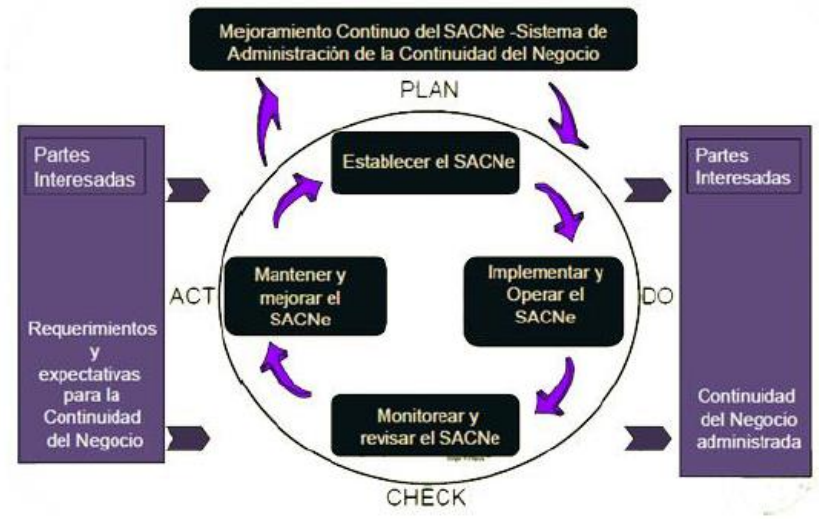


Gráfico N° 2. PDCA para un Sistema de Gestión de la Continuidad del Negocio
Fuente: (Alexander & AMBCI, 2012)

El “establecimiento” es el **Plan**. Allí se aprecian los principales requerimientos: Contexto de la Organización, Liderazgo, Planeamiento y Soporte. Las cláusulas 4, 5, 6 y 7 de la norma corresponden al establecimiento.

Seguidamente se tiene la “implementación y operación”, el cual es el **Do**; esta etapa del proceso está compuesta por los requerimientos de la cláusula 8. Contemplamos sus principales requerimientos: Planeamiento operativo y Control, Análisis de Impacto en el Negocio (BIA), Evaluación de Riesgos, Estrategias de continuidad, Procedimientos de Continuidad, Ejercicios y Pruebas.

Luego se tiene la fase “monitoreo y revisión”, la cual representa al **Check.** Allí se pueden apreciar los principales requerimientos de esta sección: Monitoreo y Medición, Análisis y Evaluación Auditoria y Revisión. Esta fase comprende los requerimientos de la cláusula 9 de la norma.

Finalmente, se tiene la fase de “mantenimiento y mejora”, representando a la fase **Act,** la cual engloba todos los requerimientos de la cláusula 10 de la norma: No conformidad y Acción Correctiva, Mejora Continua.

Gráfico N° 3. El ciclo relacionado a las cláusulas de la norma ISO 22301
Fuente: (Alexander & AMBCI, 2012)

Tabla N° 1. PDCA de la norma ISO 22301

Cláusula	Componente	Descripción
Cláusula 4	Plan	Introduce los requisitos necesarios para establecer el contexto de la BCMS tal como se aplica a la organización, así como las necesidades, requisitos y alcance.
Cláusula 5	Plan	Resume los requisitos específicos para el papel de la alta dirección en BCMS, y cómo el liderazgo articula sus expectativas a la organización a través de una declaración de política.
Cláusula 6	Plan	Describe los requisitos relacionados con el establecimiento de estrategias, objetivos y principios para el BCMS en su conjunto.
Cláusula 7	Plan	Admite operaciones BCMS en lo que se refiere al establecimiento competencia y comunicación de manera recurrente / según sea necesario con las partes interesadas, mientras documenta, controla, mantiene y retiene la documentación requerida.
Cláusula 8	Do	Define los requisitos de continuidad del negocio, determina cómo abordarlos y desarrollar los procedimientos para gestionar un incidente disruptivo.
Cláusula 9	Check	Resume los requisitos necesarios para medir el negocio. desempeño de gestión de continuidad, cumplimiento de BCMS con esta Norma Internacional y expectativas de la gerencia, y busca retroalimentación de la gerencia con respecto a las expectativas.
Cláusula 10	Act	Identifica y actúa sobre la no conformidad BCMS a través de correctivo acción.

Fuente: Adaptado de (OSI, 2010)

1.3. Definiciones conceptuales

a. **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.

b. **Grupos de interés:** Personas u organizaciones que se ven impactadas por las operaciones de una empresa. Ejemplos: clientes, socios del negocio, empleados, proveedores, accionistas, entidades gubernamentales, entre otros.

c. **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

d. **Periodo máximo tolerable de interrupción:** Es el periodo de tiempo luego del cual la viabilidad de la empresa sería afectada seriamente, si un producto o servicio en particular no es reanudado.

e. **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

f. **Riesgo:** La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.

g. **Riesgo operacional:** La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

h. **Tiempo objetivo de recuperación:** Es el tiempo establecido por la empresa para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.

II. METODOS Y MATERIALES

2.1. Formulación de la investigación

No se plantea hipótesis en la investigación, pero se formula la siguiente pregunta de investigación:

¿De qué manera un Plan de continuidad de negocio basado en la norma ISO 22301 mejora la gestión de los procesos críticos en la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque?

2.2. Tipo de investigación

Este trabajo de tesis se ha tipificado como **aplicada, descriptiva – propositiva, no experimental**.

a. La investigación es **aplicada** porque se aplican los fundamentos teóricos de la gestión de la continuidad del negocio, específicamente la ISO/IEC 22301, para el desarrollo de una propuesta metodológica que permita mejorar la gestión de la continuidad de los procesos críticos en el Gobierno Regional de Lambayeque.
b. Es de tipo **descriptiva** porque describe cada una de las fases y actividades que se proponen en la propuesta metodológica de gestión de la continuidad, definiéndose para cada una de ellas, los procedimientos, responsables y el diseño de los formatos que se van a utilizar. Detalla la situación acerca del estado actual del problema de la gestión de la continuidad de los procesos, describe sus particularidades y características, sus limitaciones y sus puntos críticos.
c. La investigación es de tipo **propositiva** por cuanto se fundamenta en una necesidad o vacío dentro de la institución que se está tomando como caso de estudio. Se realizará una propuesta de un sistema de gestión de la continuidad de los procesos crítico a nivel de propuesta y no se tiene la intención de modificar la realidad actual.
d. **No experimental**, porque no se pretende medir el efecto de la propuesta en la realidad.

2.3. Operacionalización de variables

Dado que la investigación es del tipo no experimental, el propósito de la investigación fue valorar el Plan de gestión de la continuidad propuesto en base a las siguientes dimensiones e indicadores:

Tabla N° 2. Operacionalización de las variables de la investigación

VARIABLE	DIMENSION	INDICADORES	ESCALA
Plan de continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque	Análisis de impacto en el negocio	Nivel de análisis de procesos para identificar sus roles, funciones y activos críticos, con sus correspondientes valoraciones de criticidad y tiempos máximos de caída	Categórica ordinal de 4 ítems: 1. Clave 2. Relevante 3. Estándar 4. Irrelevante
		Grado de aceptabilidad del desarrollado del BIA, para identificar y determinar los impactos operacionales, económicos y reputacionales, en la organización, en el caso de tener paralizaciones de los procesos	
	Tolerancia de riesgo organizacional	Grado de aceptabilidad de la determinación de las prioridades de recuperación de los procesos, identificando su Tiempo Objetivo de Recuperación (RTO) y su Punto Objetivo de Recuperación (RPO)	
	Evaluación de riesgos	Grado de aceptabilidad de la identificado y clasificado los activos de TI críticos que dan soporte a los procesos, para ser considerados en el análisis de riesgos de continuidad	
		Grado de aceptabilidad de la definición del criterio de priorización de los activos de TI y un procedimiento coherente para la valoración de su criticidad	
		Grado de aceptabilidad de la identificación de las amenazas que pueden afectar a los activos de TI	
		Nivel de análisis para identificar distintas clases de amenazas, como: ¿desastres naturales, desastres industriales, ataques intencionados, etc.	
		Grado de aceptabilidad de la identificación de vulnerabilidades existentes en el entorno de la organización, que podrían ser aprovechados por las amenazas para afectar a los activos de TI	
		Grado de aceptabilidad de la definición del criterio de valoración de los impactos de la caída de los activos de TI y su aplicación es suficiente y coherente	
		Grado de aceptabilidad de la definición del criterio de valoración de las probabilidades de ocurrencia de los escenarios de riesgo y su aplicación es suficiente y coherente	
		Grado de aceptabilidad de la definición del sistema de valoración para determinar el nivel de exposición a los escenarios de riesgos	
		Nivel de análisis para valorar el nivel de exposición a los riesgos en base a información suficiente y pertinente	
		Grado de aceptabilidad de la identificación de los diferentes escenarios de paralización de los procesos críticos en base a los resultados de un análisis de riesgos	
	Procedimientos de continuidad de negocio	Grado de aceptabilidad de la identificación de las acciones actuales y se han definido las acciones preventivas para los diferentes escenarios de paralización de los procesos críticos	

		Nivel de análisis para la definición de estrategias de continuidad y acciones de recuperación para los diferentes escenarios de paralización de los procesos críticos	
	Roles, responsabilidades y prioridades	Grado de aceptabilidad de la definición de una estructura organizativa de respuesta ante incidentes, con sus correspondientes roles y tiempos de actuación para llevar a cabo el Plan de continuidad	

Fuente: Elaboración propia

2.4. Método de investigación

Para la elaboración del presente trabajo de investigación se utilizaron los siguientes métodos:

a. **Descriptivo analítico y sistemático.** Este método permitió desarrollar cada uno de los componentes del Plan de gestión de la continuidad propuesto, analizando y especificando los procedimientos a seguir; así como el diseño de los formatos a utilizar. Para ello, fue necesario utilizar la investigación bibliográfica, como libros, artículos, normas y estándares relacionados a la gestión de la continuidad con el propósito de disponer de un panorama mucho más amplio del tema, que permitió efectuar un análisis a profundidad y plantear las mejoras, a través de un procedimiento metodológico sistemático y metódico.

b. **Analítico.** Porque la propuesta del Plan de gestión de la continuidad se construyó desde una perspectiva de descomposición del sistema de continuidad en fases, en base a las recomendaciones y buenas prácticas del marco de referencia tomado como guía, como es la ISO/IEC 22301.

c. **Sintético.** Una vez analizados los aspectos teóricos, se realizó una síntesis de su aplicación al problema que se aborda en la investigación, contextualizándolo a sus procesos, estructura organizativa y capacidad instalada; que facilitó en el diseño técnico y en la redacción de los componentes de la propuesta. De esta manera, se reunieron las partes del análisis realizado para llegar a la propuesta del Plan de gestión de la continuidad integrado.

d. **Deductivo**. Se utilizó para llegar a particularizar y determinar los elementos puntuales del marco teórico que fueron utilizados para definir una propuesta adecuada de Plan de gestión de la continuidad de los procesos.

e. **Estadístico.** Se empleó para la recolección de datos, tabulación, análisis e interpretación, teniendo en cuenta que el manejo de información es importante para garantizar que la información sea completa y correcta.

f. **No experimental.** Para validar el Plan de gestión de la continuidad propuesto se utilizó el método Delphi para valorar el diseño y la efectividad del Plan de Continuidad propuesto, siendo las unidades de análisis, personas que tienen responsabilidad y autoridad en el GRL sobre la gestión de la continuidad de los procesos.

Por tanto, la presente investigación es de carácter mixto porque se utilizó bibliografía e investigación de campo, para el análisis y síntesis de la situación actual; la descripción para los componentes de la propuesta a través de un procedimiento metodológico, transversal porque se tomaron datos de la situación actual, y no experimental debido a que a partir de la descripción de la problemática se desarrolló de una solución, sin someter dicha solución a ninguna prueba de experimentación.

2.5. Diseño de contrastación de hipótesis

Para responder la pregunta de la investigación se aplicó un método no experimental, conocido como método Delphi, cuyo propósito fue obtener la valoración de personas claves en la gestión de la continuidad de los procesos en el GRL, de su percepción acerca de la efectividad del diseño y operación del Plan de gestión de la continuidad propuesto, de cada uno de sus componentes (fases y actividades).

2.6. Técnicas, instrumentos, equipos y materiales de recolección de datos

Las técnicas que se utilizaron dentro del proceso de investigación para la recolección de información fueron: encuesta, entrevistas y observación directa a fin de llegar a determinar los aspectos más relevantes y los problemas que se ocasionan, así también revisión de documentación y consultas a diversas fuentes bibliográficas.

a. **La entrevista estructurada o formal**. Se lo realizó a partir de una guía prediseñada que contiene las preguntas que fueron formuladas al personal que tiene autoridad y responsabilidad en la gestión de las TI, la seguridad de la información y la gestión de la continuidad de los procesos en el GRL, para obtener la información requerida. En este caso se tuvo la guía de entrevista como instrumento para registrar las respuestas.

b. **Revisión bibliográfica y documental**. La técnica de revisión bibliográfica, fue utilizada para recopilar información teórica, en los diversos textos que abordan la temática sobre la gestión de la continuidad del negocio y la ISO 22301. Esto sirvió de soporte para la elaboración del marco teórico del estudio, también sirvió para tener conocimiento del funcionamiento de la organización objeto de análisis. Por otro lado, se recopiló documentación referente a la normativa vigente que tiene la entidad.

c. **La encuesta.** La técnica de la encuesta, se utilizó en el proceso de recolección de datos, para agrupar la opinión del personal de la OFTI, acerca de la situación actual sobre gestión de riesgos de TI, seguridad de la información y su evaluación del sistema de gestión actual. Se elaboraron, tres encuestas:
   - Evaluación del cumplimiento de la seguridad de la información (ver anexo 1)
   - Análisis de los riesgos operativos de TI (ver anexo 2)
   - Evaluación del Plan de continuidad actual (ver anexo 3)

2.7. Método para la identificación y análisis de los procesos críticos

El objetivo de esta actividad es identificar los procesos críticos a los cuales se les aplicará el Plan de gestión de la continuidad propuesto.

El método para el análisis de los procesos permite identificar los roles y funciones críticas para el GRL; así como los activos tecnológicos que le dan soporte, con la finalidad de definir los tiempos máximos tolerables de caída de los mismos. Para el fichaje de los resultados del análisis de los procesos se utilizó el siguiente formato:

<table>
<tr><th colspan="2">Nombre del proceso</th><th colspan="4">Elaboración de actividades y acciones de control</th></tr>
<tr><th colspan="2">Órgano</th><th colspan="4">Órgano de Control Institucional</th></tr>
<tr><th colspan="6">Identificación de roles y funciones críticas</th></tr>
<tr><th colspan="2">Rol</th><th colspan="4">Función crítica</th></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="2"></td><td colspan="4"></td></tr>
<tr><td colspan="2" rowspan="3"></td><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
<tr><th colspan="6">Identificación de recursos informáticos críticos en el proceso</th></tr>
<tr><th colspan="2">Tipo</th><th colspan="3">Descripción</th><th>Cantidad</th></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td></tr>
<tr><th colspan="6">Identificación de impactos de caída y tiempos aceptables de caída</th></tr>
<tr><th>Recurso</th><th colspan="2">Impacto</th><th>TMI (hh:mm)</th><th>TOR (hh:mm)</th><th>Prioridad de recupero</th></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td><td></td></tr>
</table>

2.8. Metodología para el análisis de impacto de negocio – BIA

Se definió realizar el estudio de cada uno de los procesos en 7 áreas de impacto, basadas en los campos de interés del GRL

1. Impacto financiero
2. Usuario interno
3. Usuarios externos
4. Impacto humano
5. Infraestructura física
6. Impacto legal y regulatorio
7. Impacto en imagen y reputación

Estas áreas de estudio fueron determinadas teniendo en cuenta los aspectos de importancia para el GRL, el impacto financiero que afecta directamente los intereses de la economía de la entidad, el cliente interno debido a que los procesos en su mayoría son transversales a varias áreas de la entidad, el usuario que hace referencia a las entidades con quienes se tiene convenios, el aspecto humano en relación a la importancia que tienen los trabajadores, la infraestructura física debido a que esta soporta toda la operación de la entidad, el aspecto legal y regulatorio encargado de garantizar el cumplimiento de la normatividad que controla la gestión del GRL y a su vez proporciona cumplimiento de los contratos adquiridos; finalmente, el impacto en imagen y reputación posiciona al GRL frente a la comunidad, quienes son la razón de existencia de la entidad.

La escala establecida de calificación está comprendida en el rango de uno (1) a cinco (5):

- Impacto Nivel 1: Insignificante.
- Impacto Nivel 2: Bajo.
- Impacto Nivel 3: Moderado.
- Impacto Nivel 4: Significativo.
- Impacto Nivel 5: Severo.

A continuación, se observará la evaluación aplicada para cada impacto, los efectos generados para el GRL por cada espacio de tiempo que estuviera detenido el proceso. Los espacios de tiempo, mostrados a continuación y usados en el análisis,

para el caso específico se debe definir de acuerdo a los antecedentes, las características y a la exigencia de la operación de la entidad:

- 0 a 1 hora.
- 1 a 4 horas.
- 4 a 8 horas.
- 8 a 24 horas.
- 24 a 48 horas.
- 48 a 72 horas.

Para determinar la criticidad de los procesos se tomó como referencia los siguientes criterios:

A. **Criticidad impacto financiero.** La criticidad relacionada con el impacto financiero fue determinada por la disminución de ingresos y afectación en la rentabilidad, que generaría para el GRL una posible interrupción de cada uno de los procesos analizados. Éstos se describen en la tabla siguiente:

Tabla N° 3. Criticidad impacto financiero

Ítem	Calificación	Descripción
1	Insignificante	Si el proceso no se encuentra disponible, no hay pérdidas. En general no hay afectación de los ingresos del GRL
2	Bajo	Si el proceso no se encuentra disponible, tiene algún impacto en ingresos, el cual no sería significativo y no impactaría en el presupuesto del GRL
3	Moderado	Si el proceso no se encuentra disponible, tiene un impacto moderado en los ingresos, podría afectar de forma moderada en el presupuesto del GRL
4	Significativo	Si el proceso no se encuentra disponible, tiene un impacto significativo y afecta el presupuesto del GRL, pero no afecta la sostenibilidad de la entidad
5	Severo	Si el proceso no se encuentra disponible, tiene un impacto severo generado por pérdidas financieras que afectan el presupuesto e ingresos del GRL y su continuidad de operación

Fuete: Elaboración propia

B. **Criticidad del impacto en el usuario interno.** La criticidad relacionada con el impacto al usuario interno fue determinada considerando la afectación a otras áreas; priorizando los procesos misionales del GRL, ante la posible interrupción de cada uno de los procesos analizados. Éstos se describen en la tabla siguiente:

Tabla N° 4. Criticidad del impacto en el usuario interno

Ítem	Calificación	Descripción
1	Insignificante	La interrupción del proceso no afecta a ninguna otra área o proceso del GRL
2	Bajo	La interrupción del proceso tiene por consecuencia la afectación de un proceso de apoyo o estratégico sin afectar el Core de los procesos del GRL
3	Moderado	La interrupción del proceso tiene por consecuencia la afectación de dos o más procesos de apoyo o estratégicos
4	Significativo	La interrupción del proceso tiene por consecuencia la afectación de dos o más procesos Core del GRL
5	Severo	La interrupción del proceso tiene por consecuencia la afectación de todos los procesos Core del GRL

Fuete: Elaboración propia

C. **Criticidad del impacto en usuarios externos.** La criticidad relacionada con el impacto a las entidades con las que se tiene convenio, fue determinada por el efecto de la prestación de servicios. Éstos se describen en la tabla siguiente:

Tabla N° 5. Criticidad del impacto en usuarios externos

Ítem	Calificación	Descripción
1	Insignificante	Si el proceso no está disponible no se afecta la imagen de la entidad
2	Bajo	Si el proceso no está disponible afecta la imagen de la entidad con otras entidades
3	Moderado	Si el proceso no está disponible afecta la imagen de la entidad con otras entidades más representativas
4	Significativo	Si el proceso no está disponible afecta la imagen de la entidad de manera general, generándose afectaciones a usuarios externos y otras entidades
5	Severo	Si el proceso no está disponible afecta de manera significativa las otras entidades, así como la percepción de seriedad del GRL, se presenta una afectación masiva a usuarios externos y otras entidades

Fuete: Elaboración propia

D. **Criticidad de impacto regulatorio o contractual.** La criticidad relacionada con el impacto regulatorio y contractual fue determinado considerando el incumplimiento de la regulación y las normas, ante la posible interrupción de cada uno de los procesos evaluados. Éstos se describen en la tabla siguiente:

Tabla N° 6. Criticidad impacto regulatorio o contractual

Ítem	Calificación	Descripción
1	Insignificante	Si el proceso no está disponible no se produce incumplimiento de normas, regulaciones o procesos contractuales
2	Bajo	Si el proceso no está disponible podría existir una probabilidad de que se generen incumplimientos de normas, regulaciones o procesos contractuales, pero no tiene un impacto importante con sanciones o reclamaciones
3	Moderado	Si el proceso no está disponible genera incumplimiento con regulaciones o contratos importantes, pero se puede dar el escenario de no recibir multas o sanciones significativas
4	Significativo	Si el proceso no está disponible genera sanciones y multas importantes por incumplimiento de la normatividad aplicable
5	Severo	Si el proceso no está disponible genera sanciones y multas que pueden generar pérdidas financieras

Fuete: Elaboración propia

E. **Criticidad en la imagen corporativa.** La criticidad relacionada con el impacto a la imagen corporativa fue determinada considerando el incumplimiento de los servicios hacia la comunidad, ante la posible interrupción de cada uno de los procesos analizados. Éstos se describen en la tabla siguiente:

Tabla N° 7. Criticidad impacto en la imagen corporativa

Ítem	Calificación	Descripción
1	Insignificante	Si el proceso no se encuentra disponible no afecta la imagen del GRL
2	Bajo	Si el proceso no se encuentra disponible podría afectar la imagen del GRL
3	Moderado	Si el proceso no se encuentra disponible afecta la imagen que se tiene del GRL
4	Significativo	Si el proceso no se encuentra disponible afecta la imagen del GRL significativamente
5	Severo	Si el proceso no se encuentra disponible afecta totalmente la imagen del GRL, se pierde totalmente la imagen

Fuete: Elaboración propia

F. **Criticidad en recursos humanos.** La criticidad relacionada con el recurso humano fue determinada considerando el ausentismo del personal involucrado en los procesos analizados. Éstos se describen en la tabla siguiente:

Tabla N° 8. Criticidad impacto en recursos humanos

Ítem	Calificación	Descripción
1	Insignificante	Si el personal que incurre directamente en el área para llevar a cabo los procesos siempre está disponible
2	Bajo	Si el personal que incurre directamente en el área para llevar a cabo los procesos, presenta algún inconveniente, que le impida llegar a su lugar de trabajo, pero existe un backup (persona capacitada) que realice su actividad
3	Moderado	Si el personal que incurre directamente en el área para llevar a cabo los procesos, presenta algún inconveniente, pero puede realizarlo remotamente
4	Significativo	Si el personal que incurre directamente en el área para llevar a cabo los procesos, no llega a tiempo y afecta las actividades del proceso
5	Severo	Si el personal que incurre directamente en el área para llevar a cabo los procesos, no se presente al lugar de trabajo, no puede desarrollar sus actividades remotamente y no cuenta con un backup que lo reemplace

Fuete: Elaboración propia

G. **Criticidad en la infraestructura física.** La criticidad relacionada con la Infraestructura física fue determinada considerando la disponibilidad de equipos que operen en las instalaciones del GRL, ante la posible interrupción de cada uno de los procesos analizados. Éstos se describen en la tabla siguiente:

Tabla N° 9. Criticidad impacto en la infraestructura física

Ítem	Calificación	Descripción
1	Insignificante	Funcionamiento de forma permanente de los equipos de comunicación y computación. 7 x 24.
2	Bajo	Funcionamiento de forma ininterrumpido de los equipos de comunicación y computación
3	Moderado	Funcionamiento de forma inconsistente de los equipos de comunicación y computación debido a fallas eléctricas, pero respaldado con un sistema interrumpido de energía o motor, con lo cual solo es afectada la operación por un lapso de 5 a 20 min
4	Significativo	Funcionamiento de forma temporal de los equipos de comunicación y computación debido a fallas eléctricas, inundaciones, falta de personal que opere los equipos, daños en infraestructura
5	Severo	Falla permanente en los equipos de comunicación y computación debido a terremoto, incendio o catástrofes, falta de personal que opere los equipos, daños en infraestructura y no contar con una contingencia previa

Fuete: Elaboración propia

2.9. Método para el análisis de riesgos de TI

El método de Gestión de Riesgo de TI propuesta, permitió determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Para lograr ello, se identifica y evalúa los diferentes componentes, que los diferentes estándares y metodologías estudiadas, establecen como básicos en la gestión de riesgos de TI, como: los activos de TI, las amenazas, las vulnerabilidades, los impactos y las probabilidades; y así identificar, tanto el nivel de riesgo existente como el nivel de riesgo aceptable de la entidad

El método contempla las siguientes actividades y tareas:

A. Identificación de activos de TI y definición de su criticidad

Esta actividad busca identificar los activos relevantes dentro de los procesos críticos identificados de la entidad, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

a. Identificación de activos de TI

En este punto se identificarán los activos que dan soporte a los procesos. Para ello se utilizará la clasificación propuesta por la ISO 27005:2008; específicamente la clasificación propuesta para activos de soporte de los activos primarios (procesos e información). Se podrá clasificar los activos de TI, según sus características, en los siguientes tipos:

- Dato: información que se genera, envía, recibe y gestionan dentro de la organización. Incluye los documentos que se gestionan dentro de sus procesos.
- Aplicación: software que se utilice como soporte en los procesos.
- Personal: actores que tienen posibilidades de acceso y manejo, de una u otra manera, de los activos de información.
- Servicio: servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.

- Tecnología: hardware donde se procesa, almacena o transmite la información.
- Instalación: lugar donde se alojan los activos de información. Puede estar ubicado dentro de la entidad o fuera de ella.
- Equipamiento auxiliar: activos que no se hallan definidos en ninguno de los anteriores tipos.

Para la clasificación de los activos de TI se utilizará el siguiente formato:

Tabla N° 10. Plantilla para el registro de los activos de TI por tipo de activo

N°	Tipo de activo de TI	Activo de TI
1		
2		
3		

b. Definición de la criticidad de los activos de TI identificados

Una vez inventariados los activos de TI es necesario identificar y documentar el valor que su seguridad representa para la entidad. Para ello, se asignará un conjunto de valores a cada activo teniendo en cuenta los diferentes requerimientos de seguridad que se consideren relevantes.

El valor que tienen los activos de información para una entidad en el ámbito de la seguridad puede medirse desde diversos puntos de vista. Estos puntos de vista se denominan, en el marco de este modelo, requerimientos de seguridad o dimensiones de la seguridad, los cuales están definidos en el Anexo N° 4.

La valoración se deberá realizar mediante la ponderación de las pérdidas ocasionadas para la entidad en caso de que falle o caiga el activo, debido a la materialización de una amenaza, de cada uno de los requerimientos de seguridad definidos para los diferentes activos de información, según las tablas de referencia del Anexo N° 4 en relación a: disponibilidad, integridad y confidencialidad.

Las escalas y criterios que se utilizarán para calificar cada una de las dimensiones de seguridad de TI de cada activo, se muestran en la tabla siguiente.

Tabla N° 11. Valores y criterios de referencia para la valoración de la criticidad de los activos de TI

	Valor	Criterio
Disponibilidad	**1**	No aplica/No es relevante
	2	Debe estar disponible al menos el 10% del tiempo
	3	Debe estar disponible al menos el 50% del tiempo
	4	Debe estar disponible al menos el 75% del tiempo
	5	Debe estar disponible al menos el 95% del tiempo

	Valor	Criterio
Integridad	**1**	No aplica / No es relevante
	2	No es relevante los errores que tenga o la información que falte
	3	Tiene que estar correcto y completo al menos en un 50%
	4	Tiene que estar correcto y completo al menos en un 70%
	5	Tiene que estar correcto y completo al menos en un 95%

	Valor	Criterio
Confidencialidad	**1**	No aplica / No es relevante
	2	Daños muy bajos, el incidente no trascendería del área afectada
	3	Daños bajos, el incidente no trascendería del área afectada
	4	Los daños serían relevantes, el incidente implicaría a otras áreas
	5	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas

Para la valoración de la criticidad de los activos de TI se utilizará el siguiente formato:

Tabla N° 12. Plantilla para la calificación de la criticidad de los activos de TI

N°	Activo	Criterios de seguridad			Total	Nivel de criticidad
		Confidencialidad	Integridad	Disponibilidad		
1						
2						
3						

Los niveles de criticidad de los activos de TI se obtendrán del producto de las calificaciones realizadas para cada criterio de seguridad y se clasificarán de la siguiente manera:

Tabla N° 13. Niveles de valoración de la criticidad de los activos de TI

Rango	Nivel de criticidad	Descripción
1 – 5	1	Muy bajo
6 – 10	2	Bajo
11 – 15	3	Medio
16 – 20	4	Alto
21 – 25	5	Muy alto

B. Identificación de amenazas por activo

En esta actividad caracteriza el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cuán probable es que pase. Es decir, describe las amenazas a los que el sistema está expuesto.

Para la identificación de las amenazas significativas de cada activo de TI identificado, se tomará en consideración lo siguiente:

- El tipo de activo
- Las dimensiones de seguridad con las que cada activo está relacionado
- La experiencia de la organización
- Los reportes de incidentes de seguridad

Tomando como referencia la tabla de inventario de las amenazas por activo y dimensión de seguridad de la información del Anexo N° 05 y el informe de valor de los activos de la actividad anterior, se debe obtener la relación de amenazas por cada activo de TI. Se utilizará el siguiente formato:

Tabla N° 14. Plantilla para la identificación de amenazas por activo

N°	Activo	Amenaza
1		
2		
3		

C. Identificación de vulnerabilidades por activo

En esta actividad se realiza el análisis de las deficiencias, debilidades y carencias que tiene la entidad en los diferentes procesos de TI relacionados a la protección de los activos que han sido identificados. El resultado de esta actividad permitirá determinar cuáles son las debilidades internas que pueden ser aprovechadas por las amenazas para materializarse y hacer fallar o atacar a los activos de TI.

Se identificarán las vulnerabilidades por activo, utilizando el siguiente formato:

Tabla N° 15. Plantilla para la identificación de las vulnerabilidades por cada Activo-Amenaza

N°	Activo	Amenaza	Vulnerabilidad
1	Activo 1	Amenaza 1.1	Vulnerabilidad 1.1.1
			Vulnerabilidad 1.1.2
		Amenaza 1.2	Vulnerabilidad 1.2.1
			Vulnerabilidad 1.2.2
2	Activo 2	Amenaza 2.1	Vulnerabilidad 2.1.1
			Vulnerabilidad 2.1.2
		Amenaza 2.2	Vulnerabilidad 2.2.1
			Vulnerabilidad 2.2.2
			Vulnerabilidad 2.2.3

D. Valorización del impacto y la probabilidad de ocurrencia de las amenazas

Esta actividad permitirá valorizar la materialización de cada una de las amenazas identificadas para cada activo de TI, tomando como referencia las vulnerabilidades encontradas para cada una de ellas. La valorización de las amenazas se realizará en base a la calificación de sus dos insumos principales, como son: el impacto que pueden ocasionar y la probabilidad de su ocurrencia.

Para la realización de dicha valorización, el estándar ISO 27005 propone varios ejemplos de métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada. En la propuesta, se optó por la realización de una matriz de calor, la cual tiene como criterios la probabilidad que cierta amenaza explote cierta vulnerabilidad y el impacto al negocio estimado que la ocurrencia del riesgo pueda ocasionar al negocio.

a. Estimación del impacto de una amenaza

Para la estimación del impacto de cada una de las amenazas identificadas se utilizará la siguiente tabla que define los niveles de impacto de las amenazas:

Tabla N° 16. Valoración de los niveles de impacto de una amenaza

Nivel	Impacto	Descripción
1	Insignificante	Tiene un efecto nulo o muy pequeño en los procesos
2	Menor	Afecta parcialmente las operaciones de los procesos. Paraliza servicios que no afectan directamente al usuario.
3	Moderado	Operativamente es sostenible, pero dificulta o retrasa las operaciones de los procesos. Paraliza parcialmente los servicios críticos a usuarios
4	Mayor	Paraliza la atención de servicios críticos a usuarios, debido a la caída significativa de las operaciones de los procesos
5	Catastrófico	Paraliza todas las operaciones de los procesos de la entidad

b. Estimación de la probabilidad de ocurrencia de una amenaza

Para la estimación de la probabilidad de ocurrencia de cada una de las amenazas consideradas se utilizará la siguiente tabla que define los niveles de probabilidad de ocurrencia o frecuencia de las amenazas:

Tabla N° 17. Valoración de los niveles de probabilidad de ocurrencia de una amenaza

Nivel	Probabilidad	Descripción
1	Raro	No se registra en los últimos 5 años
2	Improbable	Se podría presentar una vez cada 5 años
3	Posible	Se podría presentar una vez al año
4	Probable	Se podría presentar una vez cada mes
5	Casi seguro	Se podría presentar varias veces en el mes

E. Cálculo de los niveles de riesgos

El cálculo del nivel de riesgos intrínseco de cada una de las amenazas identificadas para cada activo, estará en función de la valoración y clasificación del impacto y la probabilidad de su ocurrencia. Se utilizará la siguiente relación:

$$NR = Probabilidad\ de\ ocurrencia\ x\ Impacto \quad \text{(formula 1)}$$

El producto de esta relación se ubicará en el siguiente mapa de calor.

Tabla N° 18. Matriz de calor para la valoración del nivel de riesgo de TI

Impacto en los procesos	Probabilidad de ocurrencia				
	Raro	Improbable	Posible	Probable	Casi seguro
Catastrófico	Bajo	Medio	Alto	Muy alto	Muy alto
Mayor	Bajo	Bajo	Medio	Alto	Muy alto
Moderado	Muy bajo	Bajo	Medio	Medio	Alto
Mínimo	Muy bajo	Bajo	Bajo	Bajo	Medio
Insignificante	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

2.10. Método para la evaluación del Plan de Continuidad propuesto

Se propone un método y una forma estructurada que permita evaluar objetivamente el diseño y la efectividad del Plan de Continuidad propuesto, en concordancia con los requerimientos, recomendaciones y buenas prácticas de la norma ISO/IEC 22301.

Es un método que permite relacionar variables cuantitativas y cualitativas a partir de los pesos asignados por las personas que tienen autoridad y desempeñan funciones de gestión de la continuidad en el GRL, con el fin de valorar objetivamente la efectividad en el diseño y la efectividad del Plan de Continuidad propuesto. Se conoce como Método Delphi. Este método fue creado por los matemáticos norteamericanos, Norman Dalkey y Olaf Hermes, en 1963, con el propósito de establecer el consenso de expertos con respecto al acontecimiento de un hecho en el futuro[1].

Con el método "Delphi" se obtendría la opinión y el conocimiento de las personas encargadas de las funciones de:

- Jefatura de OFTI
- Oficialía de Seguridad de la Información
- Jefatura de la Recursos Humanos
- Jefatura de Administración

Para su aplicación se consideró las siguientes características:

- **Anonimato:** Durante su aplicación ninguna de las personas que evalúan el Plan debe saber que otras personas también estaban evaluando el mismo. Esto

[1] El nombre "Delphi" fue escogido en memoria de la ciudad de Delfos en la antigua Grecia, que era su centro religioso en el siglo IV antes de Cristo

permitirá que ninguno de los evaluadores del Plan de Continuidad propuesto, sea influenciado por el conocimiento y experiencia de otro.

- **Iteración y realimentación controlada:** La iteración se consiguió a través de un cuestionario, elaborado específicamente para dicho fin y cuya estructura se ha tomado de los requerimientos (controles) establecidos en la norma ISO/IEC 22301. Su aplicación fue a todos los evaluadores de forma independiente.
- **Respuesta del grupo:** La información que se recopile de los evaluadores no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo obtenido.

2.10.1. Procedimiento de la evaluación del Plan de Continuidad

El procedimiento realizado fue el siguiente:

1. Se elaboró un cuestionario tomando como base las variables de la investigación, en concordancia con los requerimientos (controles) establecidos en la norma ISO/IEC 22301; de tal forma que, permita evaluar el diseño y operación del Plan de Continuidad propuesto.
2. Conseguir su compromiso de colaboración. Las personas elegidas conocen del tema y el Plan propuesto. Sin embargo, se debió socializar y explicar de forma individual al panel de personas seleccionadas, el Plan de Continuidad propuesto.
3. Se les envía a través de correo electrónico, un archivo con el cuestionario diseñado en hojas electrónicas, que contienen los niveles, factores y variables definidas a través de preguntas, para que cada uno de ellos comparta sus opiniones sobre la relevancia del Plan de Continuidad propuesto en este estudio. La asignación de la relevancia por parte del "experto", se realiza respondiendo "SÍ" o "NO" a cada factor y variable del cuestionario y la asignación de los pesos, la realiza mediante el análisis y aplicación del criterio profesional y su función dentro de la entidad, asignando o distribuyendo un peso porcentual utilizando la escala de (0% al 100%) para cada pregunta.

2.10.2. Diseño del cuestionario para la Prueba de la efectividad del diseño y operación del Plan de gestión de la continuidad propuesto

El objetivo es probar la efectividad del diseño y operación del Plan de Continuidad propuesto, en concordancia con los requerimientos (buenas prácticas) establecidos en la norma ISO/IEC 22301:2019.

Tabla N° 19. Factores y variables para probar la efectividad del diseño del Plan propuesto

Variable	Factor Relevante (indicador)	SI/NO	Peso (Madurez)
Análisis de impacto en el negocio (Business Impact Analysis-BIA): Establecer una organización identifique los procesos críticos que apoyan a sus productos y servicios claves, las interdependencias entre procesos y recursos requeridos para operar los procesos en un nivel mínimamente aceptable (Referencia: Cláusula 8: Operación, ISO/IEC 22301:2019)			
Análisis de impacto en el negocio (BIA)	¿Se ha realizado el análisis de procesos para identificar sus roles, funciones y activos críticos, con sus correspondientes valoraciones de criticidad y tiempos máximos de caída?		
	¿Se ha desarrollado el BIA, necesario para identificar y determinar los impactos operacionales, económicos y reputacionales, en la organización, en el caso de tener paralizaciones de los procesos?		
	¿Se ha identificado los recursos tecnológicos críticos para ser considerados en el Plan de gestión de la continuidad?		
Tolerancia de riesgo organizacional: Establecer objetivos de tiempo de recuperación definidos. (Referencia: Cláusula 8: Operación, ISO/IEC 22301:2019)			
RTO y RPO	¿Se ha determinado las prioridades de recuperación de los procesos, identificando su Tiempo Objetivo de Recuperación (RTO) y su Punto Objetivo de Recuperación (RPO)?		
Evaluación de riesgos: Establecer, implantar y mantener un proceso formal documentado de valoración de riesgos que identifique, analice y evalúe sistemáticamente el riesgo de incidentes que generen interrupciones en la organización (Referencia: Cláusula 8: Operación ISO/IEC 22301:2019)			
Identificación y priorización de activos	¿Se ha identificado y clasificado los activos de TI críticos que dan soporte a los procesos, para ser considerados en el análisis de riesgos de continuidad?		
	¿Se ha definido un criterio de priorización de los activos de TI y un procedimiento coherente para la valoración de su criticidad?		
Análisis de Amenazas	¿Se ha identificado las amenazas que pueden afectar a los activos de TI?		
	Se considera distintas clases de amenazas, como: ¿desastres naturales, desastres industriales, ataques intencionados, etc.?		
Análisis de Vulnerabilidades	¿Se ha realizado la identificación de vulnerabilidades existentes en el entorno de la organización, que podrían ser		

	aprovechados por las amenazas para afectar a los activos de TI?		
Análisis de Escenarios de Riesgo	¿Se ha definido un criterio de valoración de los impactos de la caída de los activos de TI y su aplicación es suficiente y coherente?		
	¿Se ha definido un criterio de valoración de las probabilidades de ocurrencia de los escenarios de riesgo y su aplicación es suficiente y coherente?		
Evaluación de Riesgos	¿Se ha definido un sistema de valoración para determinar el nivel de exposición a los escenarios de riesgos?		
	¿Se ha valorado el nivel de exposición a los riesgos en base a información suficiente y pertinente?		
Escenarios de amenazas para la continuidad	¿Se han identificado los diferentes escenarios de paralización de los procesos críticos en base a los resultados de un análisis de riesgos?		
Procedimientos de continuidad de negocio: Definición de los procedimientos para asegurar la continuidad de las actividades y la gestión de un incidente que genere una interrupción (Referencia: (Cláusula 8.4.5. ISO/IEC 22301:2019)			
Diseño del plan de continuidad	¿Se han identificado las acciones actuales y se han definido las acciones preventivas para los diferentes escenarios de paralización de los procesos críticos?		
	¿Se han definido estrategias de continuidad y acciones de recuperación para los diferentes escenarios de paralización de los procesos críticos?		
Soporte: Establecer, implementar y mantener un SGCN eficaz a través del uso de recursos apropiados para cada actividad. Solo se seleccionó personal competente en base a formaciones y servicios de soporte. (Referencia: Cláusula 7 ISO/IEC 22301:2019)			
Roles, responsabilidades y prioridades	¿Se ha definido una estructura organizativa de respuesta ante incidentes, con sus correspondientes roles y tiempos de actuación para llevar a cabo el Plan de continuidad?		

Fuente: Adecuado de la norma ISO/IEC 22301:2019

2.10.3. Sistema de evaluación del Plan de continuidad propuesto

Para valorar cada pregunta del cuestionario se utiliza la siguiente tabla de referencia, en donde se muestran las escalas que el evaluador debe tener en cuenta, para calificar cada componente del Plan de gestión de la continuidad propuesto.

Tabla N° 20. Tabla de referencia para calificar el Plan propuesto

Peso	Significado	Color
1	CLAVE	
2	RELEVANTE	
3	ESTÁNDAR	
4	IRRELEVANTE	

Leyenda:

Clave: El elemento evaluado es importante considerarlo en el Plan de continuidad del GRL, porque permitiría cumplir a cabalidad con las funciones de gestión de la continuidad en la organización, está definido en la propuesta de manera clara y coherente y cumple con los requisitos exigidos en la norma ISO/IEC 22301:2011.

Relevante: El elemento evaluado es importante considerarlo en el Plan de continuidad del GRL, porque ayudaría a cumplir con las funciones de gestión de la continuidad en la organización y cumple con los requisitos exigidos en la norma ISO/IEC 22301:2011.

Estándar: El indicador evaluado del Plan de Continuidad propuesto puede considerarse en el GRL, con algunas modificaciones y mejoras para cumplir con los requisitos exigidos en la norma ISO/IEC 22301:2011 y para que se adecúe a las funciones de la entidad.

Irrelevante: El indicador evaluado del Plan de Continuidad propuesto no cumple con los requisitos exigidos en la norma ISO/IEC 22301:2011 por lo que no podría considerase en el GRL.

III. RESULTADOS Y DISCUSIÓN

3.1. Análisis de Impacto de Negocio – BIA

3.1.1. Objetivo del BIA

El fin primario de este análisis fue determinar el impacto que ocasionaría en: Tiempo Máximo de Interrupción (TMI) y Tiempo Objetivo de Recuperación (TOR), la caída parcial o total de cada proceso que es gestionado a través de un soporte tecnológico informático o de comunicaciones, a través de la red de datos del GRL, y cuyos resultados guiarán el desarrollo de estrategias de recuperación posteriores a un evento de crisis o a la ocurrencia de una contingencia en el GRL.

3.1.2. Identificación y descripción de los procesos críticos

Para lograr el objetivo de la tarea, se aplicó un procedimiento apropiado para la recopilación de la información de los procesos a través de entrevistas, juntas de trabajo con el personal de la OFTI y el análisis de la documentación de los procesos.

a. Recopilación de información por medio de entrevistas y juntas de trabajo. Fue necesario elaborar una guía de entrevista para identificar: roles y funciones críticas, recursos informáticos críticos en el proceso, los impactos de caída; así como el tiempo aceptable de caída, a través de la definición del Tiempo Máximo de Interrupción (TMI) y Tiempo Objetivo de Recuperación (TOR) de cada recurso informático y su prioridad de recupero. Se programaron algunas nuevas entrevistas para aclarar puntos no resueltos o no claros de los proporcionados inicialmente. La información recopilada se registró en fichas técnicas, de acuerdo al diseño que se muestra en el anexo 1.
b. Recopilación de información por medio de análisis documental. Este procedimiento permitió conocer el flujo de trabajo de cada proceso con la finalidad de conocer las funciones que son soportadas por tecnologías de información.

Para este análisis, se consideraron los siguientes órganos que funcionan dentro de la Sede Regional:

- Órganos de Apoyo Administrativo
- Órgano de Control Interno
- Órgano de Defensa del Estado

Los demás órganos, no se consideraron porque funcionan en sus propios locales y cada uno de ellos debe tener su propio Plan de gestión de la continuidad.

Del análisis documental se identificó que los procesos críticos soportados por TIC que deberían ser considerados en el Plan de gestión de la continuidad de negocio, son los siguientes:

Tabla N° 21. Listado de procesos críticos gestionados a través de un soporte tecnológico informático o de comunicaciones en el GRL

Dependencia	**Procesos de Nivel 1**	
Órganos de Apoyo Administrativo	Oficina de Logística y Patrimonio – Área de Adquisiciones	Adquisición de bienes y servicios
	Oficina de Logística y Patrimonio – Unidad de Control Patrimonial	Registro de nuevas adquisiciones margesí de bienes
		Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable
		Registro y actualización de salida de bienes
	Oficina de Logística y Patrimonio – Área de Almacén	Ingreso y salida de bienes de almacén
		Percepción o recaudación de fondos
	Oficina de Contabilidad	Elaboración de obligaciones presupuestarias
	Oficina de Tesorería	Ejecución financiera de la sede presidencial del GRL
	Oficina de Recursos Humanos – Área de Remuneraciones	Elaboración de planillas para personal (activo, cesante, contratado)
	Oficina de Recursos Humanos – Área de Registro y Control	Control de asistencia y permanencia de personal
Órgano de Control Interno		Elaboración de actividades y acciones de control
Órgano de Defensa del Estado		Defensa jurídica del GRL

Elaborado por la investigadora a partir del MAPRO y otros documentos relacionados

Para cada proceso se realizó su análisis de criticidad con la finalidad de identificar los roles, funciones y recursos informáticos críticos, que deberían seguir funcionando a través de la activación del Plan de gestión de la continuidad. Para ello, se elaboraron las siguientes fichas descriptivas:

Tabla N° 22. Análisis de criticidad del proceso Elaboración de actividades y acciones de control

Nombre del proceso	**Elaboración de actividades y acciones de control**
Órgano	**Órgano de Control Institucional**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Oficina Regional de Control Institucional	El Jefe de Control Institucional designa a través de memorándums a los integrantes del equipo de auditoria
	Suscribe el Informe Preliminar conjuntamente con el auditor encargado
Unidad Orgánica	El equipo de auditoria, previa acta de instalación se inicia el trabajo de campo para determinar hallazgos si hubieran
Especialista y/o Auditor Gubernamental	Realiza la Auditoria en la Unidad Orgánica auditada
	Elabora el informe preliminar
	Rectifica las observaciones

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora	03
	Laptop	04
	Impresora láser de alto rendimiento	01
	Scanner	01
Aplicaciones informáticas	Software de Control gubernamental	05
	Sistema operativo base	07
	Software ofimático	07
Otros	Flujo eléctrico	01
	Línea telefónica digital	02
	Línea telefónica IP	01
	Línea telefónica analógica	01
	Servicio de Internet	01

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora/ Laptop	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Impresora láser	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	04:00	02:00	MEDIO
Scanner	Inconvenientes o dificultad para escanear informes o documentación relacionada al trabajo de oficina	08:00	05:00	BAJO
Software de Control gubernamental	Imposibilidad de registrar o acceder a información de los expedientes legales de control institucional seguidos por el Órgano de Control	01:00	00:45	ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	00:30	00:15	MUY ALTO
Línea telefónica digital/IP	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	01:00	00:45	ALTO

Línea telefónica analógica	Imposibilidad de comunicación con oficinas de otras Direcciones Regionales u otras instituciones	04:00	02:00	MEDIO
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Tabla N° 23. Análisis de criticidad del proceso Defensa jurídica del GRL

Nombre del proceso	**Defensa jurídica del GRL**			
Órgano	**Órgano de Defensa del Estado (Procuraduría Pública Regional)**			
Identificación de roles y funciones críticas				
Rol	**Función crítica**			
Presidencia Regional	Registra demanda contra el GRL o denuncia contra el GRL y/o Presidente Regional			
	Emite Resolución Ejecutiva Regional			
Oficina Regional de Asesoría Jurídica (ORAJ)	Elabora el informe para que autorice al PPR a iniciar las acciones judiciales			
Procurador Público Regional (PPR)	Elabora informes o impugnaciones hasta las instancias necesarias			
	Elabora informe mensual estadístico de procesos			
Identificación de recursos informáticos críticos en el proceso				
Tipo	**Descripción**		**Cantidad**	
Equipamiento	Computadora Laptop Impresora láser de alto rendimiento Scanner		02 01 01 01	
Aplicaciones informáticas	Sistema operativo base Software ofimático		03 03	
Otros	Flujo eléctrico Línea telefónica IP		01 01	
Identificación de impactos de caída y tiempos aceptables de caída				
Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora/ Laptop	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Impresora láser	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	04:00	02:00	MEDIO
Scanner	Inconvenientes o dificultad para escanear informes o documentación relacionada al trabajo de oficina	08:00	05:00	BAJO
Sistema operativo base	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	00:30	00:15	MUY ALTO
Línea telefónica IP	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	01:00	00:45	ALTO

Tabla N° 24. Análisis de criticidad del proceso Adquisición de bienes y servicios

Nombre del proceso	**Adquisición de bienes y servicios**
Órgano	**Oficina de Logística y Patrimonio – Área de Adquisiciones**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Secretaría de Adquisiciones	Registra la Solicitud de Compra y/o Solicitud de Servicio
Coordinador de Unidad de Trabajo - CUT	Determina el valor referencial, realiza el resumen ejecutivo e informe de certificación presupuestal, elabora proyecto de resolución administrativa de expediente de contratación y otros
Área de Procesos de Selección	Registra el proceso en el SEACE
	Realiza el contrato
Oficina de Planeamiento, Presupuesto y Ordenamiento Territorial (ORPPOT)	Da la Certificación Presupuestal y calendario de compromisos
Oficina Regional de Administración (ORA)	Da VºBº a las solicitudes de compra y/o Solicitudes de Servicio
Área de adquisiciones	Procede al giro de las Órdenes de compra y/o Ordenes de Servicio
	Notifica las solicitudes de compra y/o Orden de servicio al proveedores y Unidades Orgánicas involucradas en el proceso
Almacén	Recepciona y registra los bienes según la orden de compra
	Recepciona y registra la guía de remisión y factura
Oficina de Contabilidad	Procede a comprometer Órdenes
	Procede a devengar
Oficina de Tesorería	Realiza el giro y el pagado de las ordenes

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora	07
	Laptop	06
	Impresora láser de alto rendimiento	02
	Impresora de inyección de sistema continuo	11
	Scanner	01
Aplicaciones informáticas	SEACE	03
	SIGA - Módulo de Control Patrimonial	05
	Sistema operativo base	13
	Software ofimático	13
	Software visor pdf	13
Otros	Flujo eléctrico	05
	Línea telefónica digital	08
	Línea telefónica IP	03
	Línea telefónica analógica	01
	Servicio de Internet	01

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora/ Laptop	Indisponibilidad de uso de equipos	00:30	00:15	MUY ALTO
Impresora láser	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	01:00	00:45	ALTO

Scanner	Inconvenientes o dificultad para escanear informes o documentación relacionada al trabajo de oficina	02:00	01:00	ALTO
SEACE	Imposibilidad de registrar, actualizar o acceder a información de los expedientes de los procesos de adquisición de bienes y servicios (externo)	00:30	00:15	MUY ALTO
SIGA - Módulo de Control Patrimonial	Imposibilidad de registrar, actualizar o acceder a información de los expedientes de los procesos de adquisición de bienes y servicios (Interno)	00:30	00:15	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	01:00	00:45	ALTO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	01:00	00:45	ALTO
Software visor pdf	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios en formato pdf	02:00	01:00	ALTO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	00:30	00:15	MUY ALTO
Línea telefónica digital/IP	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	01:00	00:45	ALTO
Línea telefónica analógica	Imposibilidad de comunicación con oficinas de otras Direcciones Regionales u otras instituciones	01:00	00:45	ALTO
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Tabla N° 25. Análisis de criticidad del proceso Registro de nuevas adquisiciones margesí de bienes

Nombre del proceso	**Registro de nuevas adquisiciones margesí de bienes**
Órgano	**Oficina de Logística y Patrimonio – Unidad de Control Patrimonial**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Jefatura Oficina de Logística y Patrimonio	Organiza y remite las Órdenes de Compra a Responsable
Responsable de la Unidad de Control Patrimonial	Verifica que los bienes comprados estén dentro del Catálogo Nacional de Bienes
	Codifica el bien asignándole el correlativo correspondiente al bien
	Elabora el Margesí Institucional de la incorporación de todos los bienes
Almacén	Remite todas las Órdenes de Compra de Bienes a Unidad de Control Patrimonial

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora Impresora de inyección de sistema continuo	03 02
Aplicaciones informáticas	SIGA - Módulo de Control Patrimonial Sistema operativo base Software ofimático	03 03 03
Otros	Flujo eléctrico Línea telefónica digital Servicio de Internet	02 02 01

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	04:00	02:00	MEDIO
SIGA - Módulo de Control Patrimonial	Imposibilidad de registrar, actualizar o acceder a información de los expedientes de los procesos de adquisición de bienes y servicios (Interno)	01:00	00:45	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	04:00	02:00	MEDIO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	04:00	02:00	MEDIO
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Tabla N° 26. Análisis de criticidad del proceso Registro y actualización de salida de bienes

Nombre del proceso	**Registro y actualización de salida de bienes**
Órgano	**Oficina de Logística y Patrimonio – Unidad de Control Patrimonial**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Jefatura Oficina de Logística y Patrimonio	Organiza y deriva solicitud a Unidad de Control Patrimonial para su atención
Responsable de la Unidad de Control Patrimonial	Solicita a Almacén verificar la disponibilidad de los Bienes
	Elabora Formato de Salida de Bienes
	Remite documento a Unidad Orgánica con copia a Portería y Archivo
Almacén	Comunica la disponibilidad de los Bienes a la Unidad de Control Patrimonial
Unidad Orgánica solicitante	Solicita la Atención para Salida de Bien

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora Impresora de inyección de sistema continuo	03 02
Aplicaciones informáticas	Sistema operativo base Software ofimático	03 03
Otros	Flujo eléctrico Línea telefónica digital	02 02

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	04:00	02:00	MEDIO
Sistema operativo base	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	04:00	02:00	MEDIO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	04:00	02:00	MEDIO

Nota: Las Unidades Orgánicas no se consideran en el análisis del proceso en relación a los equipos informáticos críticos, porque son independientes del proceso

Tabla N° 27. Análisis de criticidad del proceso Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable

Nombre del proceso	**Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable**
Órgano	**Oficina de Logística y Patrimonio – Unidad de Control Patrimonial**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Unidad de Control Patrimonial	Comisión recopila Información de Bienes en las Unidades Orgánicas mediante trabajo de Campo
	Procesa los datos obtenidos en Trabajo de Campo
	Elabora el Inventario General de Bienes Institucionales
	Registra en el SIMI los Bienes del Inventario General en base a documentación de la Superintendencia de Bienes Nacionales
	Elabora el Acta de Conciliación con firmas

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora Impresora de inyección de sistema continuo	02 01
Aplicaciones informáticas	Software Inventario Mobiliario Institucional- SIMI Sistema operativo base Software ofimático	02 02 02
Otros	Flujo eléctrico Línea telefónica digital	01 01

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	04:00	02:00	MEDIO
Software Inventario Mobiliario Institucional-SIMI	Imposibilidad de registrar, actualizar o acceder a información de Bienes del Inventario General	01:00	00:45	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	04:00	02:00	MEDIO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	04:00	02:00	MEDIO

Tabla N° 28. Análisis de criticidad del proceso Ingreso y salida de bienes de almacén

Nombre del proceso	**Ingreso y salida de bienes de almacén**
Órgano	**Oficina de Logística y Patrimonio – Área de Almacén**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Almacén Central	Recepciona y registra mercadería según orden de compra y guía de remisión
	Elabora Planilla de Conformidad de ingreso al almacén
	Registro en Vincard y Kardex
	Despacho de Mercadería a través de POD
Almacén de Obra	Hace pedido orden de despacho y la firma
Oficina de Contabilidad	Contabiliza y da trámite para pago

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora	03
	Impresora de inyección de sistema continuo	02
Aplicaciones informáticas	SIGA - Módulo de Logística y Almacén	02
	SIGA - Módulo de Contabilidad	01
	Sistema operativo base	03
	Software ofimático	03
Otros	Flujo eléctrico	02
	Línea telefónica digital	03
	Servicio de Internet	02

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	04:00	02:00	MEDIO
SIGA - Módulo de Logística y Almacén	Imposibilidad de registrar, actualizar o acceder a información de inventarios de almacén	01:00	00:45	MUY ALTO
SIGA - Módulo de Contabilidad	Imposibilidad de registrar, actualizar o acceder a información de Contabilidad	01:00	00:45	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	04:00	02:00	MEDIO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	02:00	01:00	ALTO
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Tabla N° 29. Análisis de criticidad del proceso Ejecución financiera de la sede presidencial del GRL

Nombre del proceso	**Ejecución financiera de la sede presidencial del GRL**
Órgano	**Oficina de Tesorería**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Oficina de Tesorería	Solicita la apertura de cuentas bancarias
	Recepción de: órdenes de compra, órdenes de servicio, obligaciones presupuestarias
	Giro de Comprobantes de pago
	Giro de cheques y/o Abono Electrónico
	Ingreso de operaciones de gasto en SIAF-SP
	Deposita detracción en cuenta de Proveedor
	Gira cheque a SUNAT y se entrega comprobante de retención a proveedor
Oficina Regional de Administración	Envía requerimiento al MEF Solicitando apertura de cuentas
Oficina de Contabilidad	Tramita para VºBº previo control

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora/Laptop Impresora de inyección de sistema continuo	11 05
Aplicaciones informáticas	Sistema Integrado de Administración Financiera – SIAF SIGA - Módulo de Contabilidad Sistema operativo base Software ofimático	04 03 11 11
Otros	Flujo eléctrico Línea telefónica digital Línea telefónica IP Línea telefónica analógica Servicio de Internet	03 05 02 02 02

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora/Laptop	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	03:00	02:00	MEDIO
SIAF	Imposibilidad de registrar, actualizar o acceder a información de los procesos administrativos involucrados	01:00	00:45	MUY ALTO
SIGA - Módulo de Contabilidad	Imposibilidad de registrar, actualizar o acceder a información de Contabilidad	01:00	00:45	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de	02:00	01:00	ALTO

	adquisición de bienes y servicios			
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	02:00	01:00	ALTO
Línea telefónica analógica	Imposibilidad de comunicación con oficinas de otras Direcciones Regionales u otras instituciones	02:00	01:00	ALTO
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Tabla N° 30. Análisis de criticidad del proceso Percepción o recaudación de fondos

Nombre del proceso	**Percepción o recaudación de fondos**
Órgano	**Oficina de Tesorería**

Identificación de roles y funciones críticas	
Rol	**Función crítica**
Oficina de Tesorería	Recepción de ingresos por diversos conceptos en Caja
	Elaboración de Recibo de Ingresos
	Registro de operaciones de INGRESOS en el SIAF-SP
	Contabilización de operación de ingresos en el SIAF-SP

Identificación de recursos informáticos críticos en el proceso		
Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora/Laptop Impresora de inyección de sistema continuo	05 03
Aplicaciones informáticas	Sistema Integrado de Administración Financiera – SIAF SIGA - Módulo de Tesorería Sistema operativo base Software ofimático	03 02 05 05
Otros	Flujo eléctrico Línea telefónica digital Línea telefónica IP Servicio de Internet	01 02 01 02

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora/Laptop	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	03:00	02:00	MEDIO
SIAF	Imposibilidad de registrar, actualizar o acceder a información de los procesos administrativos involucrados	01:00	00:45	MUY ALTO
SIGA - Módulo de Tesorería	Imposibilidad de registrar, actualizar o acceder a información de Tesorería	01:00	00:45	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	02:00	01:00	ALTO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	02:00	01:00	ALTO
Línea telefónica analógica	Imposibilidad de comunicación con oficinas de otras	02:00	01:00	ALTO

	Direcciones Regionales u otras instituciones			
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Tabla N° 31. Análisis de criticidad del proceso Elaboración de obligaciones presupuestarias

Nombre del proceso	**Elaboración de obligaciones presupuestarias**
Órgano	**Oficina de Contabilidad**

Identificación de roles y funciones críticas

Rol	**Función crítica**
-Unidad Orgánica -Entidad – Convenio -Oficina de Recursos Humanos (ORH) -Sub Gerencia de Ejecución de Proyectos de Inversión	Emite: -Solicitud de Viáticos -Fondo para pagos en efectivo -Fondo fijo de caja chica -Subvenciones Otorgadas -Encargo por convenio -Valorizaciones de Obra -Planilla de Dietas -Encargos Interno -Planilla de Remuneraciones (cesantes, contratados, activos) -Planilla de Remuneraciones de Personal de Construcción Civil
Oficina de Contabilidad	Elabora Obligación Presupuestaria en base a Documentación sustentatoria
	Afecta Presupuestalmente la Obligación Presupuestaria
	Registra el compromiso en el SIAF -SP

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora/Laptop Impresora de inyección de sistema continuo	07 05
Aplicaciones informáticas	Sistema Integrado de Administración Financiera – SIAF SIGA - Módulo de Contabilidad Sistema operativo base Software ofimático	03 04 07 07
Otros	Flujo eléctrico Línea telefónica digital Línea telefónica IP Línea telefónica analógica Servicio de Internet	01 03 02 01 01

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora/Laptop	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	03:00	02:00	MEDIO
SIAF	Imposibilidad de registrar, actualizar o acceder a información de los procesos administrativos involucrados	01:00	00:45	MUY ALTO
SIGA - Módulo de Contabilidad	Imposibilidad de registrar, actualizar o acceder a información de Contabilidad	01:00	00:45	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de	02:00	01:00	ALTO

	adquisición de bienes y servicios			
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	02:00	01:00	ALTO
Línea telefónica analógica	Imposibilidad de comunicación con oficinas de otras Direcciones Regionales u otras instituciones	02:00	01:00	ALTO
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Nota: Las Unidades Orgánicas, Entidad – Convenio, Oficina de RRHH y Sub Gerencia de Ejecución de Proyectos de Inversión, no se consideran en el análisis del proceso en relación a los equipos informáticos críticos, porque son independientes del proceso

Tabla N° 32. Análisis de criticidad del proceso Elaboración de planillas para personal (activo, cesante, contratado)

Nombre del proceso	**Elaboración de planillas para personal (activo, cesante, contratado)**
Órgano	**Oficina de Recursos Humanos – Área de Remuneraciones**

Identificación de roles y funciones críticas

Rol	Función crítica
Área de Remuneraciones	Se registra incidencias
	Se ingresa Descuentos
	Se Procesa Planilla
	Se elabora la Obligación Presupuestaria
	Se elabora el PDT
Oficina de Contabilidad	Se compromete en el SIAF – SP
	Se Devenga en el SIAF-SP
Oficina de Tesorería	Realiza Envío Electrónico Vía SIAF-SP para ser pagado en el Banco de la Nación
	Gira de acuerdo a los analíticos

Identificación de recursos informáticos críticos en el proceso

Tipo	Descripción	Cantidad
Equipamiento	Computadora/Laptop Impresora de inyección de sistema continuo	06 05
Aplicaciones informáticas	Sistema Integrado de Administración Financiera – SIAF SIGA - Módulo de Planilla de Remuneraciones Sistema operativo base Software ofimático	03 03 06 06
Otros	Flujo eléctrico Línea telefónica digital Línea telefónica IP Línea telefónica analógica Servicio de Internet	01 03 02 01 03

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	Impacto	TMI (hh:mm)	TOR (hh:mm)	Prioridad de recupero
Computadora/Laptop	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	03:00	02:00	MEDIO
SIAF	Imposibilidad de registrar, actualizar o acceder a información de los procesos administrativos involucrados	01:00	00:45	MUY ALTO
SIGA - Módulo de Planilla de Remuneraciones	Imposibilidad de registrar, actualizar o acceder a información de Remuneraciones	01:00	00:45	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	02:00	01:00	ALTO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	02:00	01:00	ALTO

Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO
Línea telefónica digital	Imposibilidad de comunicación con las oficinas internas de la Sede Regional	02:00	01:00	ALTO
Línea telefónica analógica	Imposibilidad de comunicación con oficinas de otras Direcciones Regionales u otras instituciones	02:00	01:00	ALTO
Servicios de internet	Imposibilidad el acceso a las aplicaciones relacionadas con el proceso	01:00	00:45	ALTO

Tabla N° 33. Análisis de criticidad del proceso Control de asistencia y permanencia de personal

Nombre del proceso	**Control de asistencia y permanencia de personal**
Órgano	**Oficina de Recursos Humanos – Área de Registro y Control**

Identificación de roles y funciones críticas

Rol	**Función crítica**
Área de Registro y Control	Califica faltas y tardanzas
	Emite reporte diario de Asistencia
Área de Remuneraciones	Realiza descuentos de faltas y tardanzas
Trabajador	Marca su Tarjeta de asistencia

Identificación de recursos informáticos críticos en el proceso

Tipo	**Descripción**	**Cantidad**
Equipamiento	Computadora/Laptop Impresora de inyección de sistema continuo	04 02
Aplicaciones informáticas	SIGA - Sistema Integrado de Gestión Administrativa - Módulo de Control Biométrico de Personal Sistema operativo base Software ofimático	03 04 04 04
Otros	Flujo eléctrico	01

Identificación de impactos de caída y tiempos aceptables de caída

Recurso	**Impacto**	**TMI (hh:mm)**	**TOR (hh:mm)**	**Prioridad de recupero**
Computadora/Laptop	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Impresora de inyección de sistema continuo	Inconvenientes o dificultad para imprimir informes o documentación relacionada al trabajo de oficina	04:00	02:00	MEDIO
SIGA - Sistema Integrado de Gestión Administrativa - Módulo de Control Biométrico de Personal	Imposibilidad de registrar, actualizar o acceder a información de Control de Personal	02:00	01:00	MUY ALTO
Sistema operativo base	Indisponibilidad de uso de equipos	04:00	02:00	MEDIO
Software ofimático	Indisponibilidad de acceso a la documentación de los expedientes de los procesos de adquisición de bienes y servicios	04:00	02:00	MEDIO
Flujo eléctrico	Indisponibilidad de uso de equipos Indisponibilidad de acceso a la documentación de los expedientes legales y normativas	02:00	01:00	ALTO

3.1.3. Inventario de los recursos informáticos críticos

A partir de las fichas de análisis de criticidad del proceso se identificó y se elaboró el inventario de recursos informáticos críticos que fueron considerados para el análisis de riesgos posteriormente.

Las siguientes tablas muestran el inventario de activos tecnológicos informáticos de los procesos críticos considerados en el Plan de gestión de continuidad.

a. Inventario de aplicaciones informáticas críticas

Las aplicaciones informáticas identificadas son sistemas y/o módulos informáticos de propiedad únicamente del GRL, teniendo éstas el registro de las fichas pertinentes en el Instituto Nacional de Defensa de la Competencia y de la Protección de Propiedad Intelectual – INDECOPI, Filial Chiclayo, cuya documentación probatoria está en custodia de la Oficina Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial y fueron entregadas las solicitudes de Registro de Software y Base de Datos – DDA-002 por cada módulo y/o Sistema de manera independiente. La lista de los sistemas y módulos son:

Tabla N° 34. Inventario de aplicaciones informáticas críticas

Aplicación informática	Descripción
Sistema de Gestión Documentaria. SISGEDO	Efectúa el registro, control, seguimiento detallado y estricto de todos los documentos que se procesan en la Institución a nivel de trabajador y dependencia tanto externa como interna
Sistema Integrado de Gestión Administrativa - Módulo de Escalafón de Personal. SIGA – ESCALAFÓN	Está orientado a dinamizar los procesos correspondientes a registrar datos personales, laborales, familiares, estudios y otros, según la situación laboral del empleado
Sistema Integrado de Gestión Administrativa - Módulo de Gestión de Plazas Laborales. SIGA – PLAZAS	Gestiona las plazas que cuenta la Entidad, las ocupadas, presupuestadas, vacantes, y demás, y que son de base para la confeccionar de una Plantilla, donde se genera el CAP y PAP al relacionar cada plazo por órgano estructurado y trabajador nombrado
Sistema Integrado de Gestión Administrativa - Módulo de Control Presupuestal	Realiza la estimación programada de manera sistemática de las condiciones de operación y de los resultados a obtener por la Entidad en un periodo determinado
Sistema Integrado de Gestión Administrativa - Módulo de Planilla de Remuneraciones	Genera las boletas y planillas que demande la Entidad en función a lo trabajado por cada empleado público en un periodo de tiempo determinado
Sistema Integrado de Gestión Administrativa - Módulo de Control de Recaudaciones	Concierne las actividades que realiza la Entidad para obtener ingresos, a partir del cobro de bases, tributos, entre otros que constituyen prestaciones exigidas obligatoriamente para atender las necesidades, para ello se vale de la actividad financiera denominada recaudación. El Módulo Control de Recaudaciones está orientado a dinamizar los procesos de Cierre de Código de caja, Ingresos, Grupos y Sub Grupos, Horarios, Secuencias de Facturas entre otras
Sistema Integrado de Gestión Administrativa - Módulo de Logística y Almacén	Está orientado a dinamizar los procesos que demandan la apertura de los componentes, calendarios y acumulados presupuestales, los movimientos de las papeletas de compromiso y órdenes de modificación presupuestal y el proceso de actualizar acumulados
Sistema Integrado de Gestión Administrativa - Módulo de Tesorería	Está orientado a dinamizar los procesos que demandan la apertura de los componentes, calendarios y acumulados presupuestales, los movimientos de las papeletas de compromiso y órdenes de modificación presupuestal y el proceso de actualizar acumulados
Sistema Integrado de Gestión Administrativa - Módulo de Control Biométrico de Personal	Lleva el control de asistencia y permanencia del personal que labora en la Entidad, este módulo incluye una opción para registro de papeletas de salida electrónicas
Sistema Integrado de Gestión Administrativa - Módulo de Contabilidad	Se encarga de estudiar, medir y analizar el patrimonio de las empresas, con el fin de servir en la toma de decisiones y control, presentando la información, previamente registrada, de manera sistemática y útil para las distintas partes interesadas
Sistema Integrado de Gestión Administrativa - Módulo de Transparencia Pública	Posibilita subir la información para ser consultada por los ciudadanos sin requerir cuenta de acceso en cumplimiento a la Ley de Transparencia
Sistema Integrado de Gestión Administrativa - Módulo de Control Patrimonial	Está orientado a regular la administración y control de los bienes físicos y lógicos de todos los ambientes y locales que conforman el GRL, desarrollando mecanismos que permitan la eficiente gestión de los bienes. Se ha constituido un único repositorio que consolida los bienes de acuerdo al catálogo del Sistema Nacional de Bienes Estatales (SBN) contando con información segura, confiable y actualizada
Sistema Integrado de Gestión Administrativa - Módulo de Administración de Portales Web	El proceso de crear, diseñar y gestionar portales Web dinámicas se encuentra debidamente sistematizado en el Módulo Administración de Portales – SIGA, el cual permite la incorporación, mantenimiento y actualización de los portales oficiales de cada órgano Estructurados de esta Entidad
Sistema Integrado de Gestión Administrativa - Módulo de atención al usuario: “Call Center”	Asistir de manera programada y cordial al usuario interno en la solución rápida a su problema suscitado desde su misma terminal de trabajo Asistir de manera programada a los usuarios de los órganos estructurados y ciudadanos en general, vale decir que los problemas informáticos deben ser diferenciados entre “urgentes” y “prioritarios”, en ese sentido se genera un registro de atención, que va a demandar tiempo, esfuerzos, horas hombre, y productividad, variable que puede ser medida y determinar el nivel de atenciones brindadas de manera satisfactoria
Sistema Integrado de Administración Financiera - SIAF	herramienta informática que simplifica y automatiza los procesos administrativos en una entidad del Estado y que sigue las normas establecida por los Órganos Rectores de los Sistemas Administrativos del Estado:
Software de Control gubernamental	OCI Lambayeque
Programa de Declaración Telemática – PDT	PDT 600 Remuneraciones PDT 601 Planilla Electrónica PDT 65 Impuesto Selectivo al Consumo PDT 616 Trabajadores independientes PDT 617 IGV otras retenciones PDT 651 Renta Anual Personal Natural
Software Inventario Mobiliario Institucional- SIMI	Módulos de registro de bienes para la Sede Regional
SEACE	De acuerdo al convenio marco, esta Sede Regional utiliza el Módulo Web de la OSCE, denominado SEACE

b. Inventario de software crítico

En este inventario de software crítico, considera tanto el software libre como el software licenciado que cuenta el GRL. Hay que considerar que en la institución mediante normas y políticas informáticas se masificó el uso de plataformas libres en servidores, equipos informáticos, portátiles y todo elemento informático que necesite un programa de escritorio, siendo seleccionada la distribución de Debian: Ubuntu, la misma que no requiere de adquirir licencias corporativas o individuales por su uso, la autoría u otro pago a terceros. El inventario de software se muestra a continuación:

Tabla N° 35. Inventario de software libre crítico

Tipo	Nombre	Cantidad
Sistema operativo base	Ubuntu	215
Software ofimático	Libre Office 3.5	215
Software de diseño	GIMP	215
Software visor pdf	Adobe Reader	215
Software grabador	Brasero, k3b	215
Software editor	Pitivi	215
Software reproductor	VLC, Totem	215
Software navegador	Firefox, Chrome	215

Tabla N° 36. Inventario de software comercial licenciado crítico

Tipo	Nombre	Cantidad
Sistema operativo base	Windows	68
Software ofimático	Microsoft Office	45
Software de diseño	Autocad	15
Software antivirus	Nod32, Kaspersky	68

c. Inventario de equipamiento informático

A continuación, se presenta un resumen de la infraestructura tecnológica en la Sede Central, precisando que no existe ningún equipo sin marca o "ensamblado-compatible", todo equipo informático que sea propiedad del GRL debe contar con garantía de tres años del proveedor y/o fábrica

Tabla N° 37. Inventario del equipamiento informático crítico

Equipo	Cantidad
Computadora	259
Laptop	45
Servidores	7
Switch de Core (cobre)	12
Switch de borde	28
Equipo de radioenlace	6
Impresora láser de alto rendimiento	12
Impresora de inyección de sistema continuo	84
Scanner	14
Proyector	8

Nota: En el análisis de la criticidad de los procesos no se consideraron servidores, y los switch debido a que son considerados activos críticos por defecto. Por esa razón, figuran en el inventario

d. Inventario de equipamiento de comunicaciones crítico

En la sede del GRL se ha implementado una infraestructura de comunicaciones los servicios integrados de voz y datos. La telefonía es IP y brinda a todas las unidades orgánicas en la modalidad de interconexión extendida de teléfonos IP y digitales con una administración central.

La telefonía IP está basada en equipos Alcatel-Lucent, en un esquema de conectividad de troncal IP local ubicada en la Sala de Servidores de OFTI.

Tabla N° 38. Inventario del equipamiento de comunicaciones crítico

Tipo de línea	Cantidad de líneas (anexos)
Digital	124
IP	32
Analógica	2

3.1.4. Análisis del impacto en el GRL

En esta tarea se calificó el impacto que tendría una interrupción parcial o total de cada uno de los procesos considerados en el Plan de gestión de la continuidad. Para este análisis, se consideró los siguientes tipos de impactos: (1) financiero, (2) afectación al usuario interno, (3) afectación al usuario externo, (4) regulatorio/contractual, (5) imagen corporativa, (6) productividad de los RRHH y (7) en la infraestructura física.

De acuerdo a la metodología, para cada proceso crítico se realizó una valoración de impacto por franjas horarias, para cada tipo de impacto, con la finalidad de identificar los Tiempos Máximos de Interrupción tolerables (TMT) en el GRL. La escala utilizada fue de 1 a 5, siendo 1 el menor impacto y 5 el mayor.

Las siguientes tablas muestran los mapas de calor resultantes del análisis de impacto para cada proceso por tipo de impacto.

a. Valoración de los procesos en el impacto financiero

Tabla N° 39. Valoración de los procesos en el impacto financiero

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1	1	1	2	2	3
Registro de nuevas adquisiciones margesí de bienes	1	1	1	2	2	3
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1	1	2	2	3	3
Registro y actualización de salida de bienes	1	1	2	3	4	5
Ingreso y salida de bienes de almacén	1	1	2	3	4	5
Percepción o recaudación de fondos	2	3	4	5	5	5
Elaboración de obligaciones presupuestarias	2	3	4	5	5	5
Ejecución financiera de la sede presidencial del GRL	2	3	4	5	5	5
Elaboración de planillas para personal (activo, cesante, contratado)	1	1	2	2	3	3
Control de asistencia y permanencia de personal	1	1	1	1	1	2
Elaboración de actividades y acciones de control	1	1	1	1	2	2
Defensa jurídica del GRL	1	1	1	1	1	1

De la Tabla se puede observar que los procesos de “Percepción o recaudación de fondos”, “Elaboración de obligaciones presupuestarias” y “Ejecución financiera de la sede presidencial del GRL” son los que tienen un mayor impacto financiero en caso de que éste se vea paralizado por más de 8 horas, debido a que tiene relación directa con la gestión de los recursos económicos en el GRL.

b. Valoración de los procesos en el impacto de afectación al usuario interno

Tabla N° 40. Valoración de los procesos en el impacto de afectación al usuario interno

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1	1	1	2	3	3
Registro de nuevas adquisiciones margesí de bienes	1	1	1	2	3	3
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1	1	2	3	3	4
Registro y actualización de salida de bienes	1	1	3	4	4	5
Ingreso y salida de bienes de almacén	1	2	2	3	4	5
Percepción o recaudación de fondos	1	1	1	2	2	3
Elaboración de obligaciones presupuestarias	1	2	2	3	4	5
Ejecución financiera de la sede presidencial del GRL	1	2	2	3	4	5
Elaboración de planillas para personal (activo, cesante, contratado)	1	2	3	4	5	5
Control de asistencia y permanencia de personal	1	2	3	4	5	5
Elaboración de actividades y acciones de control	1	1	1	1	2	2
Defensa jurídica del GRL	1	1	2	2	3	3

La paralización de los procesos “Elaboración de planillas para personal” y “Control de asistencia y permanencia de personal” son los que general un mayor impacto en los usuarios internos del GRL, ya que la paralización parcial o total de estos procesos podrían ocasionar reclamaciones de parte de los trabajadores.

c. Valoración de los procesos en el impacto de afectación al usuario externos

Tabla N° 41. Valoración de los procesos en el impacto de afectación al usuario externo

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1	1	1	1	2	2
Registro de nuevas adquisiciones margesí de bienes	1	1	1	1	1	2
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1	1	1	1	1	2
Registro y actualización de salida de bienes	1	1	2	2	3	4
Ingreso y salida de bienes de almacén	1	1	1	2	2	3
Percepción o recaudación de fondos	1	1	2	3	4	5
Elaboración de obligaciones presupuestarias	1	1	1	2	2	3
Ejecución financiera de la sede presidencial del GRL	1	2	2	3	3	4
Elaboración de planillas para personal (activo, cesante, contratado)	1	1	1	1	1	1
Control de asistencia y permanencia de personal	1	1	1	1	1	1
Elaboración de actividades y acciones de control	1	1	2	2	3	3
Defensa jurídica del GRL	1	1	2	2	3	3

El proceso “Percepción o recaudación de fondos” es el que tiene una relación directa con los servicios que se brindan a la comunidad; es decir a los usuarios externos como personas naturales y otras instituciones. Por lo que, una afectación directa sobre este proceso, repercute directamente en los usuarios externos al dejarse de bridarles los servicios.

d. Valoración de los procesos en el impacto regulatorio/contractual

Tabla N° 42. Valoración de los procesos en el impacto regulatorio/contractual

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1	1	2	3	4	5
Registro de nuevas adquisiciones margesí de bienes	1	1	2	3	4	5
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1	1	1	1	2	2
Registro y actualización de salida de bienes	1	1	1	1	2	2
Ingreso y salida de bienes de almacén	1	1	2	2	3	4
Percepción o recaudación de fondos	1	1	2	2	3	4
Elaboración de obligaciones presupuestarias	1	1	2	2	3	4
Ejecución financiera de la sede presidencial del GRL	1	1	2	2	3	4
Elaboración de planillas para personal (activo, cesante, contratado)	1	1	1	1	1	1
Control de asistencia y permanencia de personal	1	1	1	1	1	1
Elaboración de actividades y acciones de control	1	1	1	2	2	2
Defensa jurídica del GRL	1	1	2	2	3	3

La paralización de los procesos “Adquisición de bienes y servicios” y “Registro de nuevas adquisiciones margesí de bienes” son los que potencialmente podrían generar reclamaciones, sanciones legales y multas económicas al GRL, debido a incumplimientos contractuales que podría generarse.

e. Valoración de los procesos en el impacto en imagen corporativa

Tabla N° 43. Valoración de los procesos en el impacto en imagen corporativa

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1	1	1	2	2	2
Registro de nuevas adquisiciones margesí de bienes	1	1	1	2	2	2
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1	1	1	1	1	2
Registro y actualización de salida de bienes	1	1	1	2	2	3
Ingreso y salida de bienes de almacén	1	1	2	2	3	3
Percepción o recaudación de fondos	1	2	3	3	4	5
Elaboración de obligaciones presupuestarias	1	2	3	4	5	5
Ejecución financiera de la sede presidencial del GRL	1	2	3	4	5	5
Elaboración de planillas para personal (activo, cesante, contratado)	1	1	1	1	1	2
Control de asistencia y permanencia de personal	1	1	1	1	1	1
Elaboración de actividades y acciones de control	1	2	2	3	3	4
Defensa jurídica del GRL	1	2	2	3	3	4

Los procesos “Elaboración de obligaciones presupuestarias” y “Ejecución financiera de la sede presidencial del GRL” son los que permite ejecutar obras en beneficio de terceros. La paralización de estos procesos retrasaría la ejecución de servicios y obras hacia la comunidad y podrían generar un impacto negativo significativo en la imagen institucional.

f. Valoración de los procesos en el impacto en la productividad de los RRHH

Tabla N° 44. Valoración de los procesos en el impacto en la productividad de los RRHH

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1	1	1	2	2	3
Registro de nuevas adquisiciones margesí de bienes	1	1	2	2	3	3
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1	1	2	3	3	4
Registro y actualización de salida de bienes	1	1	1	1	1	1
Ingreso y salida de bienes de almacén	1	1	2	2	3	3
Percepción o recaudación de fondos	1	1	1	1	2	2
Elaboración de obligaciones presupuestarias	1	1	1	1	1	2
Ejecución financiera de la sede presidencial del GRL	1	1	1	2	2	3
Elaboración de planillas para personal (activo, cesante, contratado)	1	1	1	1	1	2
Control de asistencia y permanencia de personal	1	1	1	2	2	3
Elaboración de actividades y acciones de control	1	1	2	3	3	4
Defensa jurídica del GRL	1	1	1	1	1	1

Las actividades e las diferentes áreas del GRL se realiza bajo un soporte informático, por lo que la inoperatividad, por ausencia del soporte informática por tiempos prologados, o la falta de control de las actividades podrían ocasionar disminución en el rendimiento de los trabajadores. Por ello, los procesos "Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable" y "Elaboración de actividades y acciones de control", son los que generarían un mayor impacto desde esta perspectiva.

g. Valoración de los procesos en el impacto en la infraestructura física

Tabla N° 45. Valoración de los procesos en el impacto en la infraestructura física

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1	2	2	3	3	4
Registro de nuevas adquisiciones margesí de bienes	1	2	2	3	4	4
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1	2	3	3	4	5
Registro y actualización de salida de bienes	1	2	3	3	4	5
Ingreso y salida de bienes de almacén	1	1	1	2	2	3
Percepción o recaudación de fondos	1	1	1	1	1	2
Elaboración de obligaciones presupuestarias	1	1	1	2	2	3
Ejecución financiera de la sede presidencial del GRL	1	1	2	3	4	4
Elaboración de planillas para personal (activo, cesante, contratado)	1	1	1	1	1	1
Control de asistencia y permanencia de personal	1	1	1	1	1	1
Elaboración de actividades y acciones de control	1	1	1	2	2	3
Defensa jurídica del GRL	1	1	1	1	1	1

La falta de oportunidad de un mantenimiento correctivo o preventivo de los equipos terminales informáticos o de la infraestructura de comunicación, que permite integrar las diferentes actividades en el GRL, la pérdida de bienes; así como las deficiencias en incorporar nuevas tecnologías, podría generar significativos impactos negativos. Por ello, los procesos “Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable” y “Registro y actualización de salida de bienes” son los que tienen mayor impacto en esta evaluación.

Ponderación de los impactos

Para determinar el nivel de criticidad de los procesos, primero se ponderó la importancia de cada uno de los impactos, asignándole un porcentaje de importancia, de la siguiente manera:

Tabla N° 46. Nivel de importancia de los tipos de impacto

Proceso	Porcentaje
financiero	20%
afectación al usuario interno	10%
afectación al usuario externo	20%
regulatorio/contractual	10%
imagen corporativa	15%
productividad de los RRHH	15%
en la infraestructura física	10%
Total	100%

La determinación de los niveles de importancia de los tipos de impacto sirvió para discriminar el impacto en el GRL, debido a que no es lo mismo valorar un impacto financiero con un impacto al usuario externo.

Para realizar la valoración de los impactos sobre cada uno de los procesos se aplicó la siguiente fórmula:

$$\Sigma(\text{Valor impacto (horas)} \times \text{Valor de porcentaje otorgado}) \qquad \text{(fórmula 1)}$$

Con esta fórmula se logró obtener el impacto real de cada proceso, en cada una de las horas establecidas. Los resultados se muestran en la tabla siguiente:

Tabla N° 47. Ponderación de impacto sobre procesos

Procesos	0 a 1 horas	1 a 4 horas	4 a 8 horas	8 a 24 horas	24 a 48 horas	48 a 72 horas
Adquisición de bienes y servicios	1.00	1.15	1.30	2.10	2.55	3.15
Registro de nuevas adquisiciones margesí de bienes	1.00	1.15	1.40	2.10	2.60	3.15
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	1.00	1.15	1.70	1.90	2.40	3.05
Registro y actualización de salida de bienes	1.00	1.15	1.90	2.30	3.00	3.75
Ingreso y salida de bienes de almacén	1.00	1.10	1.65	2.30	2.95	3.75
Percepción o recaudación de fondos	1.20	1.50	2.15	2.65	3.20	3.90
Elaboración de obligaciones presupuestarias	1.20	1.60	2.05	2.80	3.15	3.85
Ejecución financiera de la sede presidencial del GRL	1.20	1.80	2.40	3.25	3.75	4.30
Elaboración de planillas para personal (activo, cesante, contratado)	1.00	1.10	1.40	1.50	1.80	2.00
Control de asistencia y permanencia de personal	1.00	1.10	1.20	1.40	1.50	1.80
Elaboración de actividades y acciones de control	1.00	1.10	1.40	1.90	2.40	2.75
Defensa jurídica del GRL	1.00	1.10	1.55	1.65	2.10	2.20

De acuerdo al análisis se determinó que los procesos que alcanzan un mayor impacto en un tiempo más corto y los que contienen un mayor puntaje de impacto comparado con los demás procesos, son:

- Percepción o recaudación de fondos.
- Elaboración de obligaciones presupuestarias.
- Ejecución financiera de la sede presidencial del GRL.

Para cada proceso crítico se les identificó su Tiempo Objetivo de Recuperación (RTO) y su Punto Objetivo de Recuperación (RPO), de acuerdo a las necesidades del GRL.

Para determinar el RTO, se estableció el máximo nivel de riesgo tolerado por el GRL en caso de alguna emergencia o fallo en los servicios, siendo las ocho (08) horas el máximo nivel de riesgo permitido. Para estos procesos debe realizarse un plan de mitigación del riesgo mayor que a los demás, por consiguiente, el consumo

de recursos tecnológicos es mayor. Si en algún momento el GRL se enfrenta con cualquier tipo de interrupciones debe activar planes de contingencia y recuperación de las actividades críticas para evitar un impacto significativo.

Para calcular el RPO, se clasificaron las aplicaciones a las cuales se les debe hacer mecanismos de protección de datos, tales como backups o sistemas alternos. Se otorgaron valores de acuerdo a las reuniones realizadas con cada uno de los responsables.

De acuerdo al análisis, se identificaron los procesos cuyos puntos de recuperación se deben ejecutar en el menor tiempo posible, debido a que son procesos críticos para el GRL. Actualmente se realiza copias de seguridad cada 24 horas, pero existen procesos que exigen una copia cada 6 horas, por ejemplo, los procesos contables y de tesorería.

Tabla N° 48. Calculo RTO y RPO

Procesos	RTO (horas)	RPO (horas)
Adquisición de bienes y servicios	5	12
Registro de nuevas adquisiciones margesí de bienes	5	12
Inventario de bienes muebles del estado, registro y actualización de inventario del mobiliario institucional e informe de conciliación contable	5	12
Registro y actualización de salida de bienes	4	12
Ingreso y salida de bienes de almacén	4	12
Percepción o recaudación de fondos	2	6
Elaboración de obligaciones presupuestarias	2	6
Ejecución financiera de la sede presidencial del GRL	1	6
Elaboración de planillas para personal (activo, cesante, contratado)	8	24
Control de asistencia y permanencia de personal	8	24
Elaboración de actividades y acciones de control	6	12
Defensa jurídica del GRL	6	12

3.2. Análisis de riesgos de TI

3.2.1. Identificación y clasificación de los Activos de TI de los procesos

Se ha identificado los siguientes activos de TI que le dan soporte a los procesos:

Tabla N° 49. Inventario de activos de TI de los procesos

N°	ACTIVO
1	Servidor principal de dominio (DNS) Incluye: Gestión del Directorio Activo (Activity Directory)
2	Servidor principal de base de datos y aplicaciones
3	Red de comunicaciones Incluye: Firewall, gabinetes de comunicación, switch central, switch de distribución, switchs de borde
4	Sala de servidores del Centro de Procesamiento Central y del Centro de Procesamiento Alterno
5	Bases de Datos
6	Backups de base de datos
7	Personal de área de TI Incluye: racionalización, producción informática, programadores, soporte técnico y jefatura
8	Aplicaciones informáticas
9	Correo electrónico institucional
10	Equipos de cómputo terminales de ventanilla y administrativas (computadoras y laptops)
11	Código fuente de las aplicaciones Incluye: biblioteca de versiones, librerías
12	Archivos de Actas de conformidad
13	Archivo de requerimientos informáticos (físico)
14	Analistas de sistemas (responsables de la implementación de requerimientos)
15	Equipos de cómputo del Área de desarrollo de sistemas Incluye: terminales, servidor de desarrollo, laptops
16	Backups o respaldos de desarrollo y mantenimiento Incluye: código fuente, librerías
17	Herramientas de desarrollo Incluye: base de datos de desarrollo, software de desarrollo licenciado
18	Registros de control de cambios de las aplicaciones Incluye: scripts, cambios en estructuras de datos, carga de datos, manuales de usuario, pruebas realizadas
19	Backups de documentos normativos y de gestión: Incluye: reglamentaciones y procedimientos operacionales de gestión, desarrollo, calidad y seguridad), planes de TI, inventarios, contratos, etc.

Utilizando la clasificación propuesta por la ISO 27005:2008, se tiene el siguiente resultado:

Tabla N° 50. Clasificación de los activos de TI identificados

N°	Tipo de activo	Activo
1	Aplicaciones	Aplicaciones informáticas
2	Aplicaciones	Herramientas de desarrollo
3	Comunicaciones	Red de comunicaciones
4	Datos o documentos	Código fuente de las aplicaciones
5	Datos o documentos	Archivos de Actas de conformidad
6	Datos o documentos	Archivo de requerimientos informáticos (físico)
7	Datos o documentos	Registros de control de cambios de las aplicaciones
8	Equipos informáticos	Equipos de cómputo terminales de ventanilla y administrativas
9	Equipos informáticos	Equipos de cómputo del Área de Desarrollo
10	Información	Bases de Datos
11	Información	Backups de documentos normativos y de gestión
12	Instalaciones	Sala de servidores o Centro de Procesamiento Central
13	Personal	Personal de área de TI
14	Personal	Analistas de sistemas (responsables de la implementación de requerimientos)
15	Servicios	Servidor principal de dominio
16	Servicios	Servidor principal de base de datos y aplicaciones
17	Servicios	Correo electrónico institucional
18	Soporte de información	Backups de base de datos
19	Soporte de información	Backups o respaldos de desarrollo y mantenimiento

3.2.2. Definición de la criticidad de los activos de TI identificados

Una vez inventariados los activos de TI se ha valorado y clasificado su nivel de importancia o criticidad, tomando como base la calificación dada a cada característica o dimensión de seguridad de la información, de acuerdo a las escalas de valoración propuestas, obteniéndose los siguientes resultados:

Tabla N° 51. Valoración del nivel de criticidad de los activos de TI

N°	Activo	Criterios de seguridad			Prom	Nivel de criticidad
		C	I	D		
1	Servidor principal de dominio	4	5	5	4	Alto
2	Servidor principal de base de datos y aplicaciones	5	5	5	5	Muy Alto
3	Red de comunicaciones	4	1	5	3	Medio
4	Sala de servidores	4	1	5	3	Medio
5	Bases de Datos	5	5	5	5	Muy Alto
6	Backups de base de datos	5	5	5	5	Muy Alto
7	Personal de área de TI	4	1	5	3	Medio
8	Aplicaciones informáticas	4	4	5	4	Alto
9	Correo electrónico institucional	4	4	5	4	Alto
10	Equipos de cómputo terminales de ventanilla y administrativas	5	5	5	5	Muy Alto
11	Código fuente de las aplicaciones	4	5	5	4	Alto
12	Archivos de Actas de conformidad	2	3	5	3	Medio
13	Archivo de requerimientos informáticos (físico)	2	3	5	3	Medio
14	Analistas de sistemas	4	1	5	3	Medio
15	Equipos de cómputo del Área de desarrollo de sistemas	4	5	5	4	Alto
16	Backups o respaldos de desarrollo y mantenimiento	4	5	5	4	Alto
17	Herramientas de desarrollo	3	4	4	3	Medio
18	Registros de control de cambios de las aplicaciones	4	4	5	4	Alto
19	Backups de documentos normativos y de gestión:	3	3	5	3	Medio

3.2.3. Identificación de las amenazas de los Activos de TI

Para cada activo de TI se han identificado las siguientes amenazas:

Tabla N° 52. Listado de amenazas por Activo de TI

N°	Activo	Amenaza
1	Servidor principal de dominio	Paralización de procesos y actividades, no se accede a los servicios de red
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de personal y usuarios)
3	Red de comunicaciones	Paralización de servicios de comunicación
4	Sala de servidores	Sabotaje a las instalaciones
		Pérdida de Activos de TI en la sala de servidores (costo de hardware / paralización de Operaciones)
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la entidad debido a accesos inadecuados a las bases de datos
		Falta de espacio de almacenamiento

6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos
		Modificación, divulgación y destrucción de la información
8	Aplicaciones informáticas	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debidos errores en la integridad de los datos
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico por parte del proveedor
10	Equipos de cómputo terminales de ventanilla y administrativas (computadoras y laptops)	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio
11	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción.
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador
12	Archivos de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.
13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.
14	Analistas de sistemas (responsables de la implementación de requerimientos)	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software
15	Equipos de cómputo del Área de Desarrollo	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos
16	Backups o respaldos de desarrollo y mantenimiento	Reversión de adecuaciones a los sistemas, no es posible.
17	Herramientas de desarrollo	Paralización de continuidad de Desarrollo de Requerimientos
18	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente
19	Backups de documentos normativos y de gestión	Pérdida de información, Multas y/o sanciones por no cumplir con el requerimiento de información histórica por parte de ente supervisor

3.2.4. Identificación de las vulnerabilidades de los Activos de TI

Para cada relación de activo de TI - amenaza se han identificado las siguientes vulnerabilidades, el cual es el resultado del análisis de incidentes de seguridad de la información que tiene registrado:

Tabla N° 53. Listado de vulnerabilidades por Activo de TI – Amenaza

N°	Activo	Amenaza	Vulnerabilidad
1	Servidor principal de dominio	Paralización de procesos y actividades, no se accede a los servicios de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio
			Falla en los componentes físicos
			Fallas en el sistema operativo, falta de actualización de parches
			No se cuenta con un plan de mantenimiento de los servidores
			Ataque de virus
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)	Administrador tiene acceso total a la base de datos y puede realizar modificaciones
			Deficiencia en el diseño de base datos (normalización de BD).
			Usuarios acceden a servidor de base de datos por canales no autorizados
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones
			Falla de la red de comunicaciones con otras oficinas
			Fallas eléctricas que generen la interrupción de los procesos y servicios
			No se cuenta con servidor de firewall a nivel de hardware
4	Sala de servidores o Centro de Procesamiento Central	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores.
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.
		Pérdida de Activos de TI en la sala de servidores (costo de hardware / paralización de Operaciones)	No se mantiene un control o registro de acceso a las áreas restringidas
			Falta de un registro de acceso a la sala de servidores
			No se tiene una política y procedimiento para el personal que realiza mantenimiento en la institución

			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento). Y revisión de maletines.
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD
			Existencia de password no adecuados para usuarios locales y de red
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente
			Acceso a la BD desde otras aplicaciones
			Virus informáticos
			Realización de copias no autorizadas de la Base de Datos.
			Modificación no autorizada de BD
		Falta de espacio de almacenamiento	Incremento de transacciones
			No existe un procedimiento de mantenimiento de a BD.
			Incremento de espacio por virus.
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Fallas en los dispositivos de almacenamiento (disco duro del servidor)
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo
			Errores en el proceso de generación de backups
			No se lleva un registro de la generación de backups
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos	Inadecuada segregación de funciones
			No existe un plan de capacitación adecuado
			Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)
		Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos
			Falta de control y seguimiento de accesos
			Falta de acuerdos de confidencialidad

			Impulsos mezquinos que hace que el personal actúe de manera anormal en el desarrollo de sus labores
			Falta de procedimiento de mantenimiento de usuarios
8	Aplicaciones informáticas de créditos y captaciones	Paralización de procesos debido a Problemas en el procesamiento de transacciones a nivel de usuario.	Errores operativos por parte del usuario (registro de información errada)
			Fallas en las conexiones de red o en equipo de computo
			Fallas eléctricas (a partir de 2 horas).
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debidos errores en la integridad de los datos	Falta de soporte realizado a los sistemas
			No llevar un control de la historia del código fuente
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico	Problemas de conexión o servidor del servicio que brinda el proveedor
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico por parte del proveedor	No generación de copias de respaldo (cuentas creadas, permisos y configuración)
			Capacidad de almacenamiento limitada
			Borrado de cuentas por accesos no autorizados por personal que administra el correo
			Bajo nivel de complejidad de las contraseñas de correo vía acceso-página web
10	Equipos de cómputo terminales de ventanilla y analistas de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones	Personal no capacitado para el mantenimiento de equipos de computo
			No se ha determinado la vida útil de los equipos
			Incumplimiento del plan de mantenimiento de equipos.
			Fallas en sistema de alimentación eléctrica.
			Errores de configuración de los equipos
			Mal uso del equipo por parte del usuario
			Condiciones de ambientes inadecuadas
			No se tienen identificados los equipos críticos en caso de evacuación.

			El personal guarda información sensible en sus equipos y no las guarda en el servidor
11	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad
			Accesos no autorizados a la PC de Integración de Software
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema
			No complejidad de contraseñas en el respaldo de código fuente
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso
12	Archivos de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.	Registro - Inventario no adecuado de documentación
13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.	Registro - Inventario no adecuado de documentación de requerimiento
14	Analistas de sistemas (responsables de la implementación de requerimientos)	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.	Personal de desarrollo (nuevo) con poco conocimiento en todos los Procesos de Negocio
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar.
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web	Falta de monitoreo de envío y recepción de correos
			Acceso total a la Web
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software	Plan de Inducción no adecuado
15	Equipos de cómputo del Área de Desarrollo (concentra toda la información de desarrollo y de configuración de las aplicaciones)	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos	Acceso total a la Web
16	Backups o respaldos de	Reversión de adecuaciones a los sistemas, no es posible.	No se trasladan copias de respaldo en sitios alternos

	desarrollo y mantenimiento		
17	Herramientas de desarrollo	Paralización de continuidad de Desarrollo de Requerimientos	Copia de seguridad en lugares seguros
18	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente.	No identificar a los responsables de modificaciones asignadas a los analistas de sistemas.
19	Backups de documentos normativos y de gestión	Pérdida de información, Multas y/o sanciones por no cumplir con el requerimiento de información histórica por parte de ente supervisor	No se ha establecido la periodicidad para la generación de backups de la normatividad histórica.
			No se ha identificado un lugar adecuado para el resguardo de los backups

3.2.5. Valoración del impacto y probabilidad de ocurrencia de las amenazas

Para la valoración del impacto y probabilidad de ocurrencia y, en consecuencia, para obtener el nivel de riesgo al que está expuesto cada activo de TI, se realizó un levantamiento de información para evaluar los controles existentes actualmente y la efectividad de su implementación. Esta información se registra en los anexos 1, 2 y 3.

Los resultados de las valoraciones para los impactos y probabilidad de ocurrencia de cada amenaza para cada activo de TI; así como la obtención del nivel de riesgo intrínseco, se muestran en la siguiente tabla:

Tabla N° 54. Valoración del Nivel de Riesgo

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
1	Servidor principal de dominio	Paralización de procesos y actividades, no se accede a los servicios de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio	3	Moderado	2	Improbable	R1	2	Bajo
			Falla en los componentes físicos	4	Mayor	3	Posible	R2	3	Medio
			Fallas en el sistema operativo, falta de actualización de parches	5	Catastrófico	4	Probable	R3	5	Muy alto
			No se cuenta con un plan de mantenimiento de los servidores	3	Moderado	2	Improbable	R4	2	Bajo
			Ataque de virus	2	Menor	2	Improbable	R5	2	Bajo
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)	Administrador tiene acceso total a la base de datos y puede realizar modificaciones	4	Mayor	4	Probable	R6	4	Alto
			Deficiencia en el diseño de base datos (normalización de BD).	2	Menor	3	Posible	R7	2	Bajo
			Usuarios acceden a servidor de base de datos por canales no autorizados	5	Catastrófico	4	Probable	R8	5	Muy alto
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones	5	Catastrófico	3	Posible	R9	4	Alto
			Falla de la red de comunicaciones con otras oficinas	4	Mayor	4	Probable	R10	4	Alto
			Fallas eléctricas que generen la interrupción de los procesos y servicios	4	Mayor	3	Posible	R11	3	Medio

			No se cuenta con servidor de firewall a nivel de hardware	3	Moderado	2	Improbable	R12	2	Bajo
4	Sala de servidores o Centro de Procesamiento Central	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores	5	Catastrófico	2	Improbable	R13	3	Medio
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.	2	Menor	3	Posible	R41	2	Bajo
		Pérdida de Activos de TI en la sala de servidores (costo de hardware / paralización de Operaciones)	No se mantiene un control o registro de acceso a las áreas restringidas	2	Menor	2	Improbable	R15	2	Bajo
			Falta de un registro de acceso a la sala de servidores	3	Moderado	2	Improbable	R16	2	Bajo
			No se tiene una política y procedimiento para el personal que realiza mantenimiento en la institución	2	Menor	3	Posible	R17	2	Bajo
			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento). Y revisión de maletines.	4	Mayor	3	Posible	R18	3	Medio
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD	4	Mayor	3	Posible	R19	3	Medio
			Existencia de passwords no adecuados para usuarios locales y de red	3	Moderado	2	Improbable	R20	2	Bajo
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente	3	Moderado	2	Improbable	R21	2	Bajo
			Acceso a la BD desde otras aplicaciones	4	Mayor	3	Posible	R22	3	Medio

			Virus informáticos	3	Moderado	3	Posible	R23	3	Medio
			Realización de copias no autorizadas de la Base de Datos.	4	Mayor	3	Posible	R24	3	Medio
			Modificación no autorizada de BD	5	Catastrófico	4	Probable	R25	5	Muy alto
		Falta de espacio de almacenamiento	Incremento de transacciones	3	Moderado	3	Posible	R26	3	Medio
			No existe un procedimiento de mantenimiento de a BD.	3	Moderado	2	Improbable	R27	2	Bajo
			Incremento de espacio por virus.	3	Moderado	1	Raro	R28	1	Muy bajo
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Fallas en los dispositivos de almacenamiento (disco duro del servidor)	4	Mayor	3	Posible	R29	3	Medio
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo	2	Menor	2	Improbable	R30	2	Bajo
			Errores en el proceso de generación de backups	5	Catastrófico	4	Probable	R31	5	Muy alto
			No se lleva un registro de la generación de backups	3	Moderado	3	Posible	R32	3	Medio
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos	Inadecuada segregación de funciones	3	Moderado	2	Improbable	R33	2	Bajo
			No existe un plan de capacitación adecuado	2	Menor	3	Posible	R34	2	Bajo
			Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)	2	Menor	3	Posible	R35	2	Bajo
		Modificación, divulgación y	Abuso de privilegios de accesos	4	Mayor	3	Posible	R36	3	Medio
			Falta de control y seguimiento de accesos	5	Catastrófico	3	Posible	R37	4	Alto

		destrucción de la información	Falta de acuerdos de confidencialidad	4	Mayor	3	Posible	R38	3	Medio
			Impulsos mezquinos que hace que el personal actúe de manera anormal en el desarrollo de sus labores	3	Moderado	3	Posible	R39	3	Medio
			Falta de procedimiento de mantenimiento de usuarios	3	Moderado	2	Improbable	R40	2	Bajo
8	Aplicaciones informáticas	Paralización de procesos debido a Problemas en el procesamiento de transacciones a nivel de usuario	Errores operativos por parte del usuario (registro de información errada)	3	Moderado	3	Posible	R41	3	Medio
			Fallas en las conexiones de red o en equipo de computo	3	Moderado	3	Posible	R42	3	Medio
			Fallas eléctricas (a partir de 2 horas)	4	Mayor	3	Posible	R43	3	Medio
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debidos errores en la integridad de los datos	Falta de soporte realizado a los sistemas	3	Moderado	2	Improbable	R44	2	Bajo
			No llevar un control de la historia del código fuente	4	Mayor	3	Posible	R45	3	Medio
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico	Problemas de conexión o servidor del servicio que brinda el proveedor	3	Moderado	3	Posible	R46	3	Medio
		Pérdida de datos por gestión inadecuada del servidor de correo	No generación de copias de respaldo (cuentas creadas, permisos y configuración)	3	Moderado	3	Posible	R47	3	Medio
			Capacidad de almacenamiento limitada	2	Menor	2	Improbable	R48	2	Bajo

		electrónico por parte del proveedor	Borrado de cuentas por accesos no autorizados por personal que administra el correo	3	Moderado	2	Improbable	R49	2	Bajo
			Bajo nivel de complejidad de las contraseñas de correo vía acceso-página web	3	Moderado	3	Posible	R50	3	Medio
10	Equipos de cómputo terminales de ventanilla y administrativas	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio	Personal no capacitado para el mantenimiento de equipos de computo	4	Mayor	2	Improbable	R51	2	Bajo
			No se ha determinado la vida útil de los equipos	2	Menor	2	Improbable	R52	2	Bajo
			Incumplimiento del plan de mantenimiento de equipos	2	Menor	3	Posible	R53	2	Bajo
			Fallas en sistema de alimentación eléctrica	3	Moderado	3	Posible	R54	3	Medio
			Errores de configuración de los equipos	2	Menor	3	Posible	R55	2	Bajo
			Mal uso del equipo por parte del usuario	3	Moderado	4	Probable	R56	3	Medio
			Condiciones de ambientes inadecuadas	2	Menor	3	Posible	R57	2	Bajo
			No se tienen identificados los equipos críticos en caso de evacuación	3	Moderado	2	Improbable	R58	2	Bajo
			El personal guarda información sensible en sus equipos y no las guarda en el servidor	4	Mayor	4	Probable	R59	4	Alto
11	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la	No se realizan copias de seguridad	4	Mayor	2	Improbable	R60	2	Bajo
			Accesos no autorizados a la PC de Integración de Software	4	Mayor	2	Improbable	R61	2	Bajo

		versión existente en producción								
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo)	4	Mayor	3	Posible	R62	3	Medio
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema	4	Mayor	3	Posible	R63	3	Medio
			No complejidad de contraseñas en el respaldo de código fuente	3	Moderado	3	Posible	R64	3	Medio
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso	5	Catastrófico	4	Probable	R65	5	Muy alto
12	Archivos de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.	Registro - Inventario no adecuado de documentación	3	Moderado	3	Posible	R66	3	Medio
13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.	Registro - Inventario no adecuado de documentación de requerimiento	3	Moderado	3	Posible	R67	3	Medio
14	Analistas de sistemas (responsables de la implementación	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.	Personal de desarrollo (nuevo) con poco conocimiento en todos los procesos	2	Menor	4	Probable	R68	2	Bajo
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar	3	Moderado	3	Posible	R69	3	Medio

	de requerimientos)	Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web	Falta de monitoreo de envío y recepción de correos	3	Moderado	2	Improbable	R70	2	Bajo
			Acceso total a la Web	4	Mayor	3	Posible	R71	3	Medio
		Pérdida de recursos debido a Implementaciones no acordes a metodología y estándares de desarrollo de software	Plan de Inducción no adecuado	2	Menor	2	Improbable	R72	2	Bajo
15	Equipos de cómputo del Área de Desarrollo	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos	Acceso total a la Web	3	Moderado	3	Posible	R72	3	Medio
16	Backups o respaldos de desarrollo y mantenimiento	Reversión de adecuaciones a los sistemas, no es posible	No se trasladan copias de respaldo en sitios alternos	5	Catastrófico	3	Posible	R74	4	Alto
17	Herramientas de desarrollo	Paralización de continuidad de Desarrollo de Requerimientos	Copia de seguridad en lugares seguros	3	Moderado	3	Posible	R75	3	Medio
18	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente.	No identificar a los responsables de modificaciones asignadas a los analistas de sistemas.	3	Moderado	3	Posible	R76	3	Medio
19	Backups de documentos	Pérdida de información, Multas y/o sanciones por	No se ha establecido la periodicidad para la generación de backups de la normatividad histórica	3	Moderado	2	Improbable	R77	2	Bajo

	normativos y de gestión	no cumplir con el requerimiento de información histórica por parte de ente supervisor	No se ha identificado un lugar adecuado para el resguardo de los backups	2	Menor	2	Improbable	R78	2	Bajo

3.3. Diseño del plan de continuidad

De los resultados del análisis de riesgos, se identificaron los siguientes escenarios de riesgo que pueden afectar la continuidad de los procesos críticos, considerados en el Plan de gestión de la continuidad:

Tabla N° 55. Listado de escenarios de riesgos identificados

Escenario de riesgo	Tipo
Interrupción de la red	Fallas en los servidores de producción Falla de los sistemas de comunicación y enlace con las demás oficinas
Interrupción del servicio eléctrico	
Acciones malintencionadas	
Fallas en los equipos terminales	
Fallas en el software	Fallas en los sistemas de información Falla del Software operativo y de escritorio
Virus informáticos	
Seguridad de personal	Reclutamiento y contrato Salida de empleados
Robo de equipos e información	
Desastres naturales/Industriales	Incendios Terremotos Inundaciones

3.3.1. Interrupción de la red

La interrupción en la red se debe a cualquiera de las siguientes causas:

- Fallas en los servidores

a. Fallas en los servidores de producción

De manera general, el reconocimiento de las fallas de los servidores que están en producción, puede detectarse de las siguientes maneras:

- No se puede interactuar con las aplicaciones del servidor
- Mensaje de pérdida de conexión con el servidor.
- Mensaje de que los recursos compartidos con el servidor no están disponibles.
- Ping desde el servidor a cualquier otra PC no responde.
- Diagnósticos de operatividad de la tarjeta de red negativos.

Los servidores que están considerados como críticos son:

- Servidor de Base de datos
- Servidor Controlador de dominio
- Servidor de Antivirus
- Servidor Firewall
- Servidor Web
- Servidor SIAF

A continuación, se definen las acciones para enfrentar cada escenario de riesgos de este tipo:

Descripción	Al presentarse esta falla, ninguna las oficinas no podrán conectarse al servidor de Base de Datos de producción porque la arquitectura lógica de base de datos es centralizada. Es decir, las bases de datos a los que acceden las aplicaciones están alojadas en un solo servidor de datos. Por lo tanto, no podrán acceder ni disponer de la información relacionada a las diferentes aplicaciones informáticas instaladas. Las causas pueden ser: o Falla física: del disco duro, memoria RAM, los procesadores, tarjeta de red, controlador del disco o Infección de virus o Error lógico de datos, que no permite la lectura ni escritura en los archivos de bases de datos. o Indisponibilidad por sobrecalentamiento, caídas por picos de energía, incendio o inundaciones o Indisponibilidad por sabotaje o ataques malintencionados o Indisponibilidad por robo
Medidas actuales y preventivas	**Copias de respaldo** o Generar copias de seguridad física de las diferentes bases de datos de acuerdo a los procedimientos de generación de respaldos para cada caso y tiempos definidos, etiquetándolos y almacenándolos en lugares seguros fuera de la ubicación de la sala de servidores o Generar copias de seguridad física de las diferentes bases de datos de acuerdo a los procedimientos de generación de respaldos para cada caso y tiempos definidos en un servidor de respaldo. Las copias deben almacenarse en Sede del GRL definida para ese fin. **Mantenimiento preventivo** o Aplicar las acciones de mantenimiento programado de acuerdo al Plan anual de mantenimiento de equipos informáticos o Tener actualizada la lista de proveedores y contactos para el abastecimiento inmediato de repuestos en caso de ser necesario y generar protocolos de abastecimiento inmediato en los contratos. o Incluir en procedimientos de mantenimiento preventivo por parte del proveedor en los periodos de aplicación de la garantía **Pruebas periódicas** o Revisión periódica de los logs de actividad de los servidores para prevenir su mal funcionamiento en el momento de la recuperación de la información o Revisar permanentemente los sistemas de ventilación y enfriamiento y la temperatura ambiental de la Sala de Servidores, la cual se debe encontrar a 17°C promedio. Debe incluirse el mantenimiento preventivo de los sistemas de aire acondicionado de la Sala de servidores en el Plan anual de mantenimiento de equipos informáticos

	○ Realizar pruebas programadas de los sistemas de protección contra incendios, abastecimiento de energía y sistemas ininterrumpidos de energía (UPS), pozos a tierra. ○ Realizar pruebas programadas del sistema de cableado eléctrico. **Control de cambios** ○ Tener actualizado el registro de cambios físicos de los servidores. **Infección de malware** ○ Verificar permanentemente la actualización de firmas del sistema antivirus ○ Verificar mediante software el funcionamiento de los filtros del servidor Firewall en relación a detección de malware **Abastecimiento de energía** ○ Realizar verificaciones programadas de la autonomía y potencia de los UPS conectados a cada servidor ○ Realizar la limpieza anual de los pozos a tierra **Climatización de la Sala de servidores** ○ El equipo de aire acondicionado y ambiente adecuado en la Sala de Servidores que mantiene una temperatura de 17° C a 22° C, lo cual favorece su correcto funcionamiento.
Medidas correctivas o de recuperación	○ Cargar la última copia de seguridad de cada una de las bases de datos en el servidor de respaldo, mientras se corrige el problema y generar el bypass de conectividad de las aplicaciones hacia ese servidor ○ Interrumpir el fluido eléctrico focalizado si fuese necesario, hasta tener controlado y/o reparado el evento de cortocircuito ○ Comunicarse inmediatamente con los proveedores de repuestos aplicando los protocolos de abastecimiento de los convenios de contrato. ○ Cuando la falla del servidor es por Error Físico de Disco de un Servidor (Sin RAID). o Ubicar el disco malogrado. o Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área. o Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso. o Bajar el sistema y apagar el equipo. o Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición. o Restaurar el último backup, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad. o Verificación el buen estado de los sistemas. o Habilitar las entradas al sistema para los usuarios. ○ Cuando la falla del servidor es por falla en la RAM los síntomas son: o El servidor no responde correctamente, por lentitud de proceso o no rendir ante el ingreso masivo de usuarios. o Ante procesos mayores se congela el proceso. o Arroja errores con mapas de direcciones hexadecimales. Las acciones de recuperación son:

	○ Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la GRL, a menos que la dificultad apremie, cambiarlo inmediatamente. ○ Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes: ○ Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área. ○ El servidor debe estar apagado, dando un correcto apagado del sistema. ○ Ubicar las memorias malogradas. ○ Retirar las memorias malogradas y reemplazarlas por otras iguales o similares. ○ Retirar la conexión del servidor con el concentrador, ello evitará que, al encender el sistema, los usuarios ingresen. ○ Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas. ○ Probar los sistemas que están en red en diferentes estaciones. ○ Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios.

b. Falla de los sistemas de comunicación y enlace con las demás oficinas

Descripción	○
Medidas actuales y preventivas	**Abastecimiento de energía** ○ Realizar verificaciones programadas de la autonomía y potencia de los UPS conectados a cada servidor ○ Realizar la limpieza anual de los pozos a tierra
Medidas correctivas o de recuperación	○ Cargar la última copia de seguridad de cada una de las bases de datos en el servidor de respaldo, mientras se corrige el problema y generar el bypass de conectividad de las aplicaciones hacia ese servidor ○ Interrumpir el fluido eléctrico focalizado si fuese necesario, hasta tener controlado y/o reparado el evento de cortocircuito ○ Comunicarse inmediatamente con los proveedores de repuestos aplicando los protocolos de abastecimiento de los convenios de contrato.

3.3.2. Interrupción servicio de internet

Descripción	Para el servicio de Internet, se tiene un contrato el cual incluye que el proveedor brindará soporte los 365 días del año, siendo una falta grave el desabastecimiento del servicio de Internet e interrupción del mismo por un espacio mayor a seis (06) horas continuas
Medidas actuales y preventivas	**Interrupción originada por proveedores** ○ Mantener la lista de contactos del servicio técnico del proveedor ○ Solicitar al proveedor, alternativas que faciliten la pronta conexión del servicio.

	o Requerir el cumplimiento contractual del servicio **Falla de configuración** o Registrar la configuración para el funcionamiento óptimo del servicio o Llevar el registro de las configuraciones IP de asignada a cada equipo **Falla en la conexión** o Verificar trimestralmente que el recorrido del cableado y puntos de la red estén funcionando adecuadamente
Medidas correctivas o de recuperación	o Cargar la última copia de seguridad de cada una de las bases de datos en el servidor de respaldo, mientras se corrige el problema y generar el bypass de conectividad de las aplicaciones hacia ese servidor o Interrumpir el fluido eléctrico focalizado si fuese necesario, hasta tener controlado y/o reparado el evento de cortocircuito o Comunicarse inmediatamente con los proveedores de repuestos aplicando los protocolos de abastecimiento de los convenios de contrato.

3.3.3. Interrupción del servicio eléctrico

Descripción	Para que funcionen adecuadamente, las computadoras personales necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible. Estas fallas eléctricas, se dan por cortes de electricidad por la parte de la Empresa de Electronorte S.A., trayendo como consecuencia que los servidores, los equipos de comunicaciones, las estaciones de trabajo y los UPS se apaguen. La sede del GRL cuenta con una planta eléctrica que entra a funcionar en 3 minutos después de la falla de eléctrica de Electronorte. GRL posee dos UPS, una de 2.2 KVA que soporta el Área de Operaciones de TI y otra de 7 KVA que soporta la Sala de Servidores, la autonomía de ambas es de aproximadamente 20 minutos. El tiempo puede aumentar si se apagan equipos de menor relevancia para la realización de las operaciones inmediatas.
Medidas actuales y preventivas	**Sistema de cableado eléctrico** o GRL cuenta con una red eléctrica estabilizada, estabilizador de estado sólido trifásico de 21 KVA y un tablero manual trifásico by pass, este regulador de tensión permite que los circuitos que, a partir de una tensión rectificada, produzcan tensión de salida estable frente a posibles variaciones de la tensión. o Establecer un contrato formal de generación eléctrica con el proveedor del servicio en el área de ubicación del GRL. o Se cuenta con proveedores, en caso de requerir reemplazo de los equipos eléctricos y de ser posible contar con repuestos.

	o Asegurar la disponibilidad del proveedor para alquilar equipos de emergencia las 24 horas del día durante la semana o incluso fines de semana. **Operación de equipos** o Apagado de los equipos eléctricos delicados tales como computadoras y equipos cuando no están operativos. **Servicio de abastecimiento contingente** o Asegurar el abastecimiento de combustibles para los grupos electrógenos. o Contar con el servicio de electricista (independiente o afiliado al proveedor principal) para poner operativo cualquier problema relacionado con el grupo electrógeno. o Almacenar linternas y baterías en un lugar fijo de la institución. **Mantenimiento y monitoreo de equipos** o Monitorear constantemente el estado del trasformador principal del GRL. o Ubicar los UPS en un lugar limpio y seco, y mantener un flujo de aire no limitado. El área donde están ubicados los UPS no está sujeta a la contaminación de polvo, gases corrosivos, exceso de humedad, vapor de aceite u otras sustancias combustibles. o Limpieza de los UPS aspirando periódicamente los depósitos de polvo alrededor de las rejillas de ventilación y limpiando la unidad con un paño seco. **Tablero de Control** o El tablero de control está diseñado de acuerdo al voltaje y corriente que soporta, y está equipado con los dispositivos necesarios de protección contra fallas (térmicos) para proteger al generador de daños, cuando hay fallas o sobrecargas en el sistema. o Limpieza con paños secos y aire comprimido, especialmente en los lugares donde se ha juntado tierra y no se puede llegar con el paño. o El polvo y la tierra pueden quitarse con una escobilla de cerdas y luego aspirar. No usar escobilla de alambre. o Inspeccionar que no haya conexiones sueltas o contaminadas. **Pozos a tierra** o Se cuenta con Tomas a Tierra o Puestas a Tierra (4 pozos siendo su valor promedio entre 1.4 y 2.8 ohmio). Estas conexiones a tierra se han realizado en base a varillas de 5/8, 1 5/8, los cuales están enterrados en tierra de humedad. Las inspecciones y mediciones de resistencia a tierra se realizan trimestralmente, con el fin de comprobar la resistencia y las conexiones, es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables. **Extensiones eléctricas y capacidades** o El uso de extensiones eléctricas debe ser controlado por los responsables de Soporte Técnico. No solo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. o Las extensiones eléctricas se encuentran fuera de la las zonas de paso, siempre que sea posible. o Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

	o Las tomas de corrientes de pared como las extensiones eléctricas deben tener toma a tierra.
Medidas correctivas o de recuperación	**Actividades durante de la interrupción** o Monitorear el UPS para programar acciones mayores. o Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso o Seguir los procedimientos adecuados para poner en funcionamiento los grupos electrógenos. o Si se cuentan con equipos UPS, grabar la información importante en las computadoras, y cerrar apropiadamente las aplicaciones y los sistemas. o Usar linternas en lugar de velas para reducir el riesgo de incendios o Apagar todos los equipos que consumen más energía que se encontraban encendidos antes de la interrupción, para prevenir sobrecargas cuando el servicio sea restablecido. **Actividades después de la interrupción** o Brindar un tiempo prudencial (depende de la magnitud de la contingencia) para restablecer los equipos activos y servicios. o Restablecer los equipos activos y servicios que se apagaron, en forma paulatina. o Validar el correcto funcionamiento de los equipos activos y servicios o Identificar los posibles daños de los equipos activos. o Notificar a los usuarios afectados el restablecimiento de los servicios y su condición. o Evaluar los daños de los equipos activos, UPS y canalizarlos a las áreas involucradas. o En el caso de una interrupción prolongada del servicio, evaluar la reubicación temporal de su puesto de trabajo. o Preparar un informe, detallando las causas, daños y recomendaciones para evitar posibles situaciones similares.

3.3.4. Acciones malintencionadas

Descripción	El GRL tiene perfilado a los usuarios de TI en base a sus funciones que realiza y cada perfil está asociado a un nivel de acceso. Sin embargo, existente intenciones no autorizadas o mal intencionadas de transacciones no autorizadas que podrían causar daños físicos o lógicos en los sistemas de información de la institución.
Medidas actuales y preventivas	**Deshonestidad** o Programar actividades de capacitación y concientización a los usuarios para el cumplimiento de las políticas y reglamentos operativos de seguridad de la información. o Evaluación permanente del trabajo del personal técnico de la OFTI. o Todos los accesos a los sistemas y aplicaciones deben realizarse mediante la identificación previa de los usuarios a través de un código de usuario y una contraseña, y a partir del log in, debe registrarse su actuación en los o bitácoras de seguimiento. o Se debe generar perfiles de usuario en base a las funciones y tareas que desarrolla en el GRL, de tal forma que sólo tengan

	acceso a las aplicaciones que le son permitidas desde un terminal determinado. La asignación de perfiles de usuario y niveles de acceso se determina por funciones en coordinación de los jefes de cada área. o Toda la información de los desarrolladores y analistas de los sistemas, tiene acceso restringido (si es posible encriptado). o Se establecen procedimientos, los cuales permiten ejercer control efectivo sobre el uso o modificación de los programas o archivos por el personal técnico. o Revisar permanentemente las bitácoras de seguimiento para determinar intenciones de acceso no autorizado.
Medidas correctivas o de recuperación	o Identificar acciones malintencionadas a través de los registros de las bitácoras de seguimiento de usuarios. o Aplicar las sanciones administrativas correspondientes a los usuarios que incumplen los reglamentos operativos y políticas de seguridad de la información. o Reestablecer la data original cuando ésta ha sido modificada y eliminada sin autorización a través de los registros de bitácora de seguimiento de usuarios.

3.3.5. Fallas en los equipos terminales

Descripción	Los equipos terminales informáticos son las PC, laptops, impresoras o scanners que los usuarios de las diferentes áreas del GRL utilizan para desarrollar su trabajo. Estos equipos pueden tener desperfectos de funcionamiento por error humano, obsolescencia, o por un agente externo como picos de energía eléctrica.
Medidas actuales y preventivas	**Falla en las PC/Laptop** o Existe un Programa de mantenimiento preventivo de los equipos de cómputo de manera trimestral. o Se cuenta con fuentes de alimentación para los equipos de cómputo, los cuales ayudan a soportar anomalías del suministro eléctrico. Para ellos contamos con: red estabilizada, supresores de picos, estabilizadores, sistemas de alimentación ininterrumpida (UPS), el sistema UPS con el que contamos, es un equipo Monofásico de doble conversión de 7 KVA de 15 a 20 minutos de autonomía y un transformador de aislamiento de 2.5 KVA. **Inventario de equipos** o Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución. operación que debe realizarse al menos anualmente. o Los equipos terminales informáticos están etiquetados de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo, etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso). (Solo equipos la OFTI). o Mantener un stock mínimo de accesorios más frecuentemente usados para minimizar la tardanza en la reposición de piezas en mal estado.

	o Mantener PC's en forma de respaldo (mínimo 2) **Uso de equipos** o Capacitar a los usuarios para el uso correcto de las PC. Incluir la capacitación en el Programa anual de actividades de la OFTI o Mensualmente se genera una copia de respaldo de la información que se almacena en cada computadora. La copia de respaldo se almacena durante un mes en un equipo informático administrado por la OFTI. **Proveedores** o Mantener comunicación directa con el servicio técnico de los proveedores de los equipos.
Medidas correctivas o de recuperación	o Las fallas del equipo pueden deberse al mal funcionamiento o a la pérdida de configuración de los mismos. Por lo que, se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo o de la pérdida de su configuración y determinar la acción correctiva a seguir. o En el caso de que el equipo con falla no tenga solución inmediata, se instala un equipo de respaldo que hay en stock, mientras que se recupera el equipo original. En este equipo se carga la última copia de respaldo generada a partir de ese equipo.

3.3.6. Fallas en el software

Descripción	Las fallas del software es uno de los escenarios de riesgo más frecuentes. Las fallas pueden ser de las aplicaciones informáticas o sistemas de información que usa el GRL en sus diferentes áreas o en el software base para el funcionamiento de los equipos informáticos, como es el sistema operativo y el software de ofimática.
Medidas actuales y preventivas	**Fallas en los sistemas de información** o El desarrollo de los sistemas o la modificación de los sistemas en producción, se realizan mediante lenguajes de programación comerciales los cuales permiten obtener características necesarias de seguridad, flexibilidad y performance. o Se cuenta con un Programa de capacitación anual del uso correcto de los sistemas. o En caso de incidentes con las aplicaciones informáticas existe un procedimiento de gestión de incidentes, mediante el cual el usuario afectado avisa y detalla el incidente para activar el protocolo de atención correspondiente. o Para el caso de las solicitudes de cambio, existe un protocolo de Requerimientos para cambios en los sistemas en producción, el cual detalla el cambio solicitado y la autorización del jefe de área. o Se cuenta con respaldos de todos los sistemas; así como un historial de cambios, manuales de usuario, en caso se necesario usarlo. **Falla del Software operativo y de escritorio** o La actualización del sistema operativo se realiza en todas las PCS uniformemente, cuando hay actualizaciones. o Todo software de escritorio instalado, es compatible con los sistemas operativos, los cuales permiten el manejo de documentos de texto, hojas de cálculo y presentaciones.

	○ Se disponen de discos de arranque de los sistemas operativos ○ Para cualquier programa que se desee ejecutar en las estaciones de trabajo, es obligatoria la autorización y asistencia del área de TI, los programas a instalar deben de contar con licencia correspondiente.
Medidas correctivas o de recuperación	○ Para las solicitudes de cambios se sigue el protocolo de atención de Requerimientos para cambios en los sistemas en producción, el cual contempla, actualizar scrips, manuales de usuario, gestión de cambios, carga de nueva data. ○ En el caso de falla de una aplicación informática, se reinstala la aplicación a partir de las copias de respaldo con los que se cuenta.

3.3.7. Virus informáticos

Descripción	Los dos medios más frecuentes para la propagación de los virus son los correos electrónicos y el uso del Internet.
Medidas actuales y preventivas	○ Se cuenta con un Software Antivirus corporativo, el cual es un contrato anual para su actualización. ○ Se debe evita que las licencias no expiren, se requiere la renovación de contrato anualmente. ○ Todo software, es manejado por personal de la OFTI, quienes son los encargados de su instalación en las PC's con su respectivo software y licencias respectivas. Las actualizaciones de los mismos, suceden normalmente al momento de prender el equipo al inicio de la jornada de trabajo. ○ Se tiene un programa permanente de bloqueo acciones como cambiar configuraciones de red, acceso a los servidores, etc. El cual se viene cumpliendo a través de políticas de usuarios. ○ Se tiene instalado el antivirus de red y en estaciones de trabajo. Antes de LOGEAR una maquina a la red (dominio) se comprueba a la existencia de virus en la PC. ○ Se tiene prohibido la descarga de archivos desde Internet, especialmente y con extensiones *.EXE, *.COM, *.BAT. Está política está configurado en el servidor firewall del GRL. ○ Mantener una estricta política respecto al acceso al PC, controlado a través del servidor controlador de dominio. ○ Mantener una política de respaldo periódico (backup) de la información almacenada en el sistema (información que no puede restablecerse a partir de documentos y otras fuentes). ○ Se ha establecido como regla en los puertos USB, la revisión contra virus antes de hacer una transferencia de información entre el ordenador y dichas unidades removibles. ○ Evitar, en la medida de lo posible, la copia de archivos o programas de compañeros o lugares en donde se conoce de antemano, que es muy posible que existan virus. ○ En el Programa de capacitación anual sobre seguridad de la información, se tiene contemplado el tema de Malware y las acciones preventivas que deben ejecutar los usuarios.
Medidas correctivas o de recuperación	○ Eliminar el virus es desactivar el restaurador de sistemas por lo que existen algunos virus que son capaces de restaurarse inmediatamente después de cada reinicio de la PC.. Por lo que la primera acción de recuperación de un equipo contra infección de virus es cambiar en las propiedades de MI PC casilla de

	desactivar restaurar sistema o desactivar restaurar sistema en todas las unidades. o Reiniciar la PC en modo a prueba de fallos (tecla superior F8 al momento que está cargando el sistema operativo) después de esto debemos pasar el antivirus. o Preparar un informe, detallando las causas y recomendaciones para evitar posibles situaciones similares. o Evaluar el desempeño actual del antivirus, en caso fuera necesario realizar cambio, verificando la correcta actualización de los mismos a través del escaneo vía Internet. o Asegurar que todo el personal esté informado del virus que pueden haber infectado sus equipos.

3.3.8. Seguridad del personal

Descripción	La seguridad del personal en el GRL, se da mediante dos puntos fundamentales en el ciclo de vida del empleado: El inicio de su actividad en la institución y la finalización de la misma. La salida de un trabajador es un punto crítico de riesgo para el GRL. En casos de problemas laborales y despidos, un trabajador modelo hasta la fecha, puede convertirse en una seria amenaza. La historia reciente está plagada de casos de sabotaje o substracción de información por parte de empleados "disgustados".
Medidas actuales y preventivas	**Reclutamiento y contrato** o Ante la incorporación de un nuevo empleado, se asigna una serie de tareas y responsabilidades proporcionando los medios materiales y la información necesaria para que pueda llevarlas a cabo. Para ello, se considera lo siguiente: o Definición del perfil de usuario del nuevo empleado. Con ello, se le asigna un código de usuario y una clave inicial de acuerdo a la función que va a cumplir y el equipo que va a utilizar. o Se firma un Acta de Acuerdo de Confidencialidad, donde el nuevo trabajador conoce de los equipos que se le entrega bajo su responsabilidad, la información que utilizará determinando sus niveles de acceso: pública y restringida. o Recibe el manual de normativa interna y firma el compromiso de cumplimiento del mismo. Este trámite establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente. o Se realiza sesiones de inducción a los nuevos trabajadores sobre el uso de los sistemas, políticas de seguridad y gestión de incidentes de TI. También se explica la normativa interna. De este modo todo empleado conoce sus obligaciones de seguridad tales como la protección de sus claves de acceso, uso adecuado del mail e Internet, clasificación de la información, etc. o Los accesos a la información y sistemas informáticos son solicitados siempre por el responsable directo del trabajador a la OFTI. Dichos accesos deben ser siempre justificables por la labor que se va a realizar, y en caso de ser privilegiados, la OFTI debe aprobar su concesión.

Medidas correctivas o de recuperación	**Salida de empleados** o Recursos Humanos lleva a cabo un procedimiento de desvinculación del personal mediante una solicitud "Solicitud de Alta, Baja y Modificación de Usuarios en los Aplicativos y Servicios Informáticos", en la cual informa el motivo por el cual ha dejado de laborar en el GRL y de esta manera se lleva una política de desvinculación del personal a través de la cual se quitan los permisos al usuario (Correos electrónicos, aplicaciones informáticas, acceso a la red, etc.). Con esto se disminuye el riesgo de ataques malintencionados por insatisfacción con la decisión de GRL. o Clasificación de las bajas: El jefe de la OFTI junto con Recursos Humanos deben clasificar la baja según las circunstancias que la rodean, en cualquiera de los tres niveles siguientes: o Baja normal, si se produce en circunstancias normales y sin conflictos. o Baja cautelar, si se produce en circunstancias normales, pero con la que hay que tener una vigilancia especial en los accesos y documentación que obra en poder del empleado: personal con acceso a información sensible, administradores de sistemas, etc. o Baja crítica si se produce en circunstancias especiales: despidos, problemas con el empleado, etc. o Gestión de las bajas: TI debe coordinar que la baja se produzca en el plazo adecuado dependiendo de la clasificación (por ejemplo, una baja crítica debe realizarse de forma inmediata). Debe efectuarse la retirada de: o accesos físicos (llaves, cajas fuertes, llaves electrónicas) o accesos lógicos (mail, acceso a la red y servidores, etc.) o material y equipamiento del GRL (portátil, móvil, etc.) o realización de copias de seguridad de la información sensible o supervisión de los accesos hasta el día de la baja o cancelación preventiva de los accesos más críticos

3.3.9. Robo de equipos e información

Descripción	El conocimiento de las señales y los métodos de robo ayudarán a los jefes de área a estar más conscientes de posibles problemas.
Medidas actuales y preventivas	o Existe una política corporativa de seguridad de la información, formalmente aprobada y difundida entre todo el personal del GRL. o Se han establecido niveles de clasificación de la información dentro del GRL ya sea digital o en papel. o Se cuenta con un Programa de capacitación anual sobre la política de seguridad de la información y seguridad para los empleados. o Existe un personal de vigilancia en los principales accesos a las instalaciones las 24 horas. La salida de un equipo informático es registrada por el personal de la oficina y por el personal de seguridad en turno, mediante boletas de entradas/salidas o Hay restricción de acceso a ciertos puntos del edifico consideradas como zonas de acceso restringido.

	○ No se permitirá que los equipos salgan de las instalaciones sin la solicitud de un previo permiso y la aplicación del procedimiento administrativo correspondiente. ○ Se cuenta con sistemas de seguridad tales como cámaras de video y tarjetas magnéticas. ○ Se han instalado elementos de seguridad a todos los recursos informáticos tales como firewalls, routers de seguridad, etc. ○ Se ha limitado el acceso a documentos y archivos electrónicos importantes del GRL al mínimo número de empleados, restringiéndolos de acuerdo a las labores realizadas por el personal y mantener un registro de todos los empleados que tienen acceso a información importante. ○ Se incluye en los Programas de capacitación de usuarios temas como el uso apropiado de las computadoras, enfatizando la importancia de mantener seguros los passwords y cerrar las aplicaciones del sistema al término de un día de trabajo. ○ El acceso a las aplicaciones informáticas y a la red de datos se realiza identificando y autenticando al usuario a través de su código de usuario y password. Adicionalmente se registra las acciones del usuario en los sistemas, en bitácoras de seguimiento. ○ En caso de extravió de algún equipo existe un procedimiento para informar inmediatamente al administrador, para que este proceda a rastrearlo.
Medidas correctivas o de recuperación	○ Determinar si la situación que se viene desarrollando es realmente un robo de equipo o de información. ○ Informar a la autoridad correspondiente dentro de la organización. ○ Informar a autoridades regulatorias cuando es un requerimiento legal. ○ Evitar la divulgación del robo descubierto entre los demás empleados. ○ Si ocurrió una intrusión a las instalaciones, no mover nada y dar aviso inmediatamente a la policía. ○ Cambiar todas las combinaciones de puertas y reemplazar candados que hayan sido dañados. ○ Revisar si los controles de acceso y elementos de seguridad usados actualmente necesitan actualizarse o tienen que adquirirse elementos adicionales. ○ Si fueron robados documentos o archivos importantes, verificar en el registro a las personas que tenían acceso a ellos. ○ Hacer un inventario de todos los documentos y archivos robados. ○ Recuperar las copias de respaldo de toda la documentación y archivos robados del sitio alterno. ○ Determinar si es necesario cambiar todos los passwords y agregar más medidas de seguridad al sistema. ○ Indicar al personal que captó cualquier actividad sospechosa previa al robo informe de esto a la policía y a las autoridades de la organización para poder hacer una adecuada reconstrucción de los hechos. ○ Preparar un informe, detallando las causas, daños y recomendaciones para evitar posibles situaciones similares.

3.3.10. Desastres naturales/industriales

Descripción	Uno de los escenarios de riesgos que tiene poca frecuencia de ocurrencia, pero que podría ocasionar un gran impacto negativo en el GRL son los desastres naturales o industriales, como: incendios, terremotos, inundaciones (éste último porque estamos en una región afectada permanentemente por el fenómeno de El Niño). Sobre este escenario de riesgos, la política de seguridad del GRL pretende, primero proteger la vida humana y luego los activos de la institución.
Medidas actuales y preventivas	**Incendio** o Estar siempre alerta. La mejor manera de evitar los incendios, es la prevención. o Todo contacto o interruptor eléctrico tiene su tapa debidamente aislada. o Se evita y monitorea conexiones de múltiples dispositivos en el mismo tomacorriente o en la misma línea de alimentación de electricidad. o Se realizan pruebas de verificación del estado de extintores y de la ubicación de cada uno de ellos según los materiales de combustión que puedan afectar a las instalaciones. o Se han colocado extintores en las principales zonas del GRL en lugares visibles, verificando periódicamente su funcionamiento y asegurar que los empleados conozcan su ubicación o Se ha incluido dentro del Programa de capacitación anual el entrenamiento para el uso y correcta manipulación de extintores, asignando responsables en cada área en caso sea necesario. o Se ha realizado inspecciones en las diferentes oficinas y ambientes del GRL para asegurar que los líquidos inflamables estén en zonas adecuadas, ventiladas y seguras, en recipientes irrompibles con una etiqueta que indique su contenido. o Se ha realizado verificaciones de las instalaciones por el personal del departamento de bomberos y defensa civil. o Se realizan simulacros dos veces por año para verificar que cada persona conoce sus responsabilidades en caso de una evacuación. o Se ha realizado verificaciones del sistema de cableado eléctrico en todas las oficinas para identificar cables perforados o con peladuras. o Se ha definido y señalizado rutas seguras de escape para el personal. o Se ha Seleccionado personal clave para coordinar las comunicaciones entre empleados. o Una política de seguridad determina que todo empleado, antes de salir de las instalaciones de GRL, deberá revisar que los aparatos eléctricos estén apagados o perfectamente desconectados. o En todas las oficinas existe y está ubicado en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín.

	Terremoto o Evaluar la calidad de las edificaciones, esto con el fin de tomar medidas para reforzarlos en caso de que sea necesario. o Tener preparado botiquín de primeros auxilios, linternas, radio a pilas, pilas, etc. y algunas provisiones en cada oficina del GRL, y que sea conocido por todos los empleados. o Tener un directorio telefónico para, en caso de necesidad, poder llamar a Protección Civil, Bomberos, Policía. o No colocar objetos pesados encima de muebles altos, asegúrelos en el suelo. o Obtener información acerca de la actividad sísmica del área en la que se ubica el GRL, para poder manejar mejor los riesgos. o Almacenar elementos químicos peligroso en lugares seguros y apropiados o Contar con un grupo electrógeno de emergencia. o Inventariar los principales equipos para establecer los procedimientos de reemplazo, pasado el terremoto. o Almacenar información vital fuera del local principal. o Formar equipos de emergencia que abarquen los principales aspectos o Promover programas de educación para el personal, así como la realización de simulacros periódicos o Señalar rutas de evacuaciones principales y alternas y zonas de seguridad para el personal. o Establecer adecuados canales de comunicación entre empleados. o Mantener un stock de emergencia de elementos como agua, alimentos, primeros auxilios, radios, linternas, guantes, etc. o Capacitar al personal y realizar pruebas de contingencia para verificar el adecuado comportamiento del personal en situaciones críticas. **Inundación** o Para evitar problemas con inundaciones ubicar los servidores a un promedio de 10 cm. de altura. o En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura. o Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado. o Cuando el daño ha sido menor se procede: o Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. o Recoger los respaldos de datos, programas, manuales y claves. (Responsable Administrador de Redes). o Instalar el sistema operativo. (Responsable Jefe de Producción). o Restaurar la información de las bases de datos y programas. (responsable encargado de Desarrollo de sistemas). o Revisar y probar la integridad de los datos. (responsable encargado de Desarrollo de sistemas).
Medidas correctivas o de recuperación	**Incendios** o En caso de que el incendio se produzca se debe evitar que el fuego se extienda rápida y libremente, es decir solamente deberá causar el menor daño posible.

	○ Se ha inducido al personal para que active la señal de alarma general del GRL y notifique inmediatamente cuando se detecta un incendio y para que siga el siguiente procedimiento: ○ Si el incendio es pequeño, trate de apagarlo, de ser posible con un extintor, teniendo en cuenta su forma de uso. Si el fuego es de origen eléctrico no intente apagarlo con agua. ○ Cuando se escuchen las sirenas de alarma todo el personal deberá abandonar inmediatamente las instalaciones donde se encuentre, además, cogerán el extintor que tenga más próximo (para ello deberá conocer la ubicación de todos ellos). ○ Conserve la calma: no grite, no corra, no empuje. Puede provocar un pánico generalizado. A veces este tipo de situaciones causan más muertes que el mismo incendio. ○ Busque salidas y señales de emergencia, las cuales deben estar indicadas con los letreros correspondientes, haciendo uso de éstas sin pánico, no corra a fin de que no provoque accidentes a otras personas que desalojan el área de siniestro. ○ En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es). ○ Si la puerta es la única salida, verifique que la chapa no esté caliente antes de abrirla; si lo está, lo más probable es que haya fuego al otro lado de ella, no la abra. ○ En caso de que el fuego obstruya las salidas, no se desespere y colóquese en el sitio más seguro. Espere a ser rescatado. ○ Si el fuego tiende a extenderse, solicite la presencia de Bomberos, para ello se dispondrá en lugares visibles los números telefónicos de emergencias, a efectos de obtener una pronta respuesta al acontecimiento. ○ La brigada de emergencia realizará, instruirá e implementará el plan de respuestas ante emergencias de fuego acorde a las características del área comprometida. ○ La supervisión del área deberá evacuar a todo el personal ajeno a la emergencia, destinándolo a lugares seguros preestablecidos (Puntos de reunión). ○ No abrir puertas ni ventanas, porque con el aire el fuego se extiende. ○ Diríjase a la puerta de salida que esté más alejada del fuego. En caso de que el fuego obstruya las salidas, no se desespere y aléjese lo más posible de las llamas, procure bloquear totalmente la entrada del humo tapando las rendijas con trapos húmedos y llame la atención sobre su presencia para ser auxiliado a la brevedad. ○ En el caso de que exista humo, no abandonar el lugar erguido, gatear o arrastrarse con un paño en la boca y nariz. Es muy importante tener memorizadas las salidas de todas las áreas del GRL, para encontrarlas incluso a oscuras. ○ Si el incendio afecta el local y la densidad del humo le permite salir, respire a través de una prenda mojada y diríjase a la calle rápidamente, pero sin correr.

	○ Si al abrir la puerta percibe gran cantidad de humo y elevada temperatura, ciérrela, acuda a la ventana que dé a la calle o a un lugar aireado y hágase ver para proceder a su rescate. ○ Si se incendia su ropa o la ropa de otra persona, ruede por el suelo o tape rápidamente con un material grueso (manta) para apagar el fuego. ○ En caso ocurra, ayude a salir a los niños, ancianos y personas con discapacidad. ○ Al llegar los bomberos o las brigadas de auxilio, infórmeles si dentro hay personas atrapadas. ○ No pase al área del siniestro hasta que las autoridades lo determinen. ○ Espere el diagnóstico de las autoridades y los expertos para poder entrar a los ambientes del GRL. ○ Si existen dudas sobre el estado de las instalaciones después del fuego, espere que las autoridades indicaran si se puede ingresar. ○ Solicitar la revisión mediante un técnico, las instalaciones eléctricas antes de conectar nuevamente la corriente. ○ Realizar labores de rescate de personas si las hubiese brindándoles los primeros auxilios de ser el caso o transportándolas al centro médico más cercano. ○ Evaluar los daños ocasionados al entorno del GRL, así como evaluar las pérdidas sufridas a nivel humano, de infraestructuras y patrimonial. ○ Si el incendio ocurrió solo en un área del local del GRL, cerrar esta área y reubicar al personal y a los equipos. ○ Hacer un inventario de todos los equipos y productos que fueron dañados. Llevar un registro de los daños para estimar las pérdidas y hacer gestiones con los seguros. ○ No encender las computadoras no otro equipo eléctrico. ○ Evaluar si es necesario trasladarse a un sitio alterno. ○ Mantener al personal informado de las condiciones del local. ○ Preparar un informe, detallando las causas, daños y recomendaciones para evitar posibles situaciones similares. **Terremotos** ○ Conservar la serenidad y evitar el pánico e histeria general ○ Ubicarse en lugares seguros previamente establecidos, de no lograrlo ubicarse bajo mesas, pupitres o escritorios alejados de ventanas u objetos que puedan caer ○ Mantente alejado de ventanas y objetos de vidrio. ○ Colocarse en el piso con las rodillas juntas y la espalda hacia las ventanas ○ Sujetar ambas manos fuertemente detrás de la cabeza, cubriéndose con ellas el cuello ○ Esconder el rostro entre los brazos para proteger la cabeza, cerrar fuertemente los ojos. ○ Si es necesario evacuar el lugar, siempre utilizando las escaleras y no ascensores. ○ No te demores yendo por tus cosas de valor. Las cosas materiales se pueden reemplazar, las personas NO.

	o Active el plan de emergencia. o Revisa tus heridas y las de los demás. Aplica primeros auxilios de ser necesario. o Al finalizar el movimiento, desaloje con prontitud y en orden a las personas que necesiten de tu ayuda. o Dirigirse a las zonas de protección ya establecidas, sin perder la calma. o Utiliza el radio a pilas y no abuses del celular. o No reingreses a un edificio dañado. o Realizar una inspección integral de las instalaciones en coordinación con las autoridades locales y compañías de seguros. o Identificar los daños producidos de las instalaciones, equipos, sistemas de comunicación, etc. o Identificar qué servicios deben contratarse para llevar cabo las reparaciones y restauraciones. Estimar costos de reparación y cronogramas de los mismos. o Establecer un área temporal para ubicar los residuos y escombros que se vayan limpiando. o Remover todos los materiales que puedan ser peligrosos y activar procedimientos de descontaminación si fuera necesario. o Asegurar a que los sistemas de protección contra incendios estén funcionando. o Si se cuenta con un sitio alterno, comunicar la dirección y los números telefónicos a todo el personal. o Informar a los usuarios a los horarios de atención, lugares de atención y cambios en los servicios y procedimientos. o Preparar un informe, detallando los daños y recomendaciones para asegurar el adecuado funcionamiento de las operaciones.

3.4. Organización de la gestión de la crisis: Roles, responsabilidades y prioridades

Para la organización de la gestión de la crisis, se propone la siguiente estructura organizativa:

Posición:	Posición o Rol perteneciente al grupo de Comunicación en Crisis
Prioridad:	Orden de importancia de las posiciones. 1 es el primero en ejecutar, 2 es el segundo.
Criticidad:	Determina si es una posición crítica/indispensable dentro del Grupo. S=Sí, N=No crítico.

Grupo:	**Equipo de Gestión de Crisis**	
Descripción:	Responsable de administrar las herramientas de comunicación predefinidas para el manejo de situaciones de crisis	
Posición / Rol	**Prioridad**	**Crítico (S/N)**
Coordinador de Gestión en Crisis	1	S
Voceros Nivel 1	1	S
Voceros Nivel 2	1	S
Voceros Nivel 3	1	S

3.4.1. Actividades de preparación, respuesta, activación y, de restauración y retorno

a. Coordinador de gestión de crisis

Grupo:	**Equipo de Gestión en Crisis**	
Rol:	**Coordinador de Gestión en Crisis**	
Nro	**Tarea, descripción**	**Frecuencia o Duración**
1.	**Actividades de Preparación (ANTES)**	
1.1.	Verificar si se cuenta con los recursos necesarios	00:10
1.2.	Realizar simulacros de Gestión en Crisis, con el personal seleccionado	01:00
2.	**Actividades de Respuesta (DURANTE)**	
2.1.	Definir las actividades necesarias para escalar el evento catalogado como ALERTA DE DESASTRE y luego de la evaluación correspondiente decidir si se declara el evento como DESASTRE	01:00
2.2.	A solicitud del Director del Comité de Crisis activar el Plan de Gestión en Crisis	Inmediato
2.3.	Establecer el Centro de Comunicación de Crisis de acuerdo al Plan de Gestión en Crisis	01:00
2.4.	Establecer voceros y realizar comunicaciones a personas interesadas, de acuerdo con Plan de Comunicación en Crisis	00:30
3.	**Activación (DESPUÉS)**	
3.1.	Definir las actividades a ser efectuadas luego de declarar el evento como DESASTRE	00:30
3.2.	Si el Plan de Gestión de Comunicación en Crisis aún no ha sido activado a solicitud del Director del Comité de crisis, activarlo	Inmediato

4.	**Operación en Contingencia (DESPUES)**	
4.1.	Definir las actividades a ser efectuadas para realizar la operación diaria de la Institución en situación de contingencia, de ser necesario, soportada por el ambiente ALTERNO	00:30
4.2.	Distribuir comunicados entre el personal del GRL	00:20
4.3.	Efectuar notificaciones relacionadas con cada situación del desastre a las personas interesadas según Plan de Gestión de Crisis y en concordancia con las decisiones del Director de Gestión de Crisis	00:30
5.	**Restauración (DESPUES)**	
5.1.	Definir las actividades a ser efectuadas para realizar la reparación de los daños ocurridos al ambiente NORMAL y la preparación al retorno a la normalidad	N.A.
5.2.	Efectuar notificaciones relacionadas con cada situación del desastre a las personas interesadas según Plan de Comunicación de Crisis y en concordancia con las decisiones del Director de Gestión de Crisis	00:30
6.	**Retorno o vuelta a la normalidad (DESPUES)**	
6.1.	Definir las actividades a ser efectuadas para realizar el retorno a la normalidad, lo que implica desactivar el ambiente ALTERNO y activar el ambiente NORMAL	N.A.
6.2.	Efectuar las comunicaciones necesarias de acuerdo con el Plan de Gestión de Crisis	N.A.
6.3.	Efectuar sesión de Lecciones Aprendidas	02:00

b. Rol: Voceros Nivel 1 (Entidades Supervisoras)

Grupo:	**Equipo de Gestión en Crisis**	
Rol:	**Voceros Nivel 1**	
Nro	**Tarea, descripción**	**Frecuencia o Duración**
1.	**Actividades de Preparación (ANTES)**	
1.1.	Definir las actividades necesarias para tener los diferentes tipos de comunicado “listos” en caso ocurra un evento catalogado como DESASTRE	N.A.
1.2.	Participar en los simulacros de comunicación en crisis cuando se le es convocado	01:00
2.	**Actividades de Respuesta (DURANTE)**	
2.1.	Definir las actividades necesarias para escalar el evento catalogado como ALERTA DE DESASTRE y luego de la evaluación correspondiente decidir si se declara el evento como DESASTRE	00:30
2.2.	Asistir a la convocatoria realizada por el Coordinador de Gestión en Crisis	Inmediato
2.3.	Dirigirse al área de acción que se le es asignada	00:20
2.4.	Participar en las personas dirigidas a las Entidades Supervisoras, de acuerdo con el Plan de Gestión en Crisis.	Diaria
3.	**Activación (DESPUÉS)**	
3.1.	Definir los comunicados a ser liberados luego de declarar el evento como DESASTRE	00:15
3.2.	Efectuar las comunicaciones necesarias de acuerdo con el Plan de Gestión de Crisis	00:20
4.	**Operación en Contingencia (DESPUES)**	
4.1.	Definir las actividades a ser efectuadas para realizar el monitoreo de las personas dirigidas a Entidades Supervisoras e informar según corresponda.	00:30

4.2.	Efectuar las comunicaciones necesarias de acuerdo con el Plan de Gestión de Crisis, y mantener informado al Coordinador de Gestión en Crisis, la evolución de la situación.	Inmediato
5.	**Restauración (DESPUES)**	
5.1.	Definir las actividades a ser efectuadas para realizar el monitoreo de las personas dirigidas a Entidades Supervisoras e informar según corresponda.	N.A.
5.2.	Transmitir al personal las decisiones distribuidas por el Coordinador de Gestión en Crisis, y comunicar actividades a realizar a los roles del personal correspondiente.	00:20
6.	**Retorno o vuelta a la normalidad (DESPUES)**	
6.1.	Definir los comunicados a ser liberados para realizar el retorno a la normalidad.	N.A.
6.2.	Participar en sesión de labores aprendidas.	02:00

c. Rol: Voceros Nivel 2 (Público en General)

Grupo:	**Equipo de Gestión en Crisis**	
Rol:	**Voceros Nivel 2**	
Nro.	**Tarea, descripción**	**Frecuencia o Duración**
1.	**Actividades de Preparación (ANTES)**	
1.1.	Definir las actividades necesarias para tener los diferentes tipos de comunicado “listos” en caso ocurra un evento catalogado como DESASTRE	N.A.
1.2.	Participar en los simulacros de comunicación en crisis cuando se le es convocado.	01:00
2.	**Actividades de Respuesta (DURANTE)**	
2.1.	Definir las actividades necesarias para escalar el evento catalogado como ALERTA DE DESASTRE y luego de la evaluación correspondiente decidir si se declara el evento como DESASTRE	00:30
2.2.	Asistir a la convocatoria realizada por el Coordinador de Gestión en Crisis	Inmediato
2.3.	Dirigirse al área de acción que se le es asignada	00:20
2.4.	Participar en las personas dirigidas al Público en General, de acuerdo con el Plan de Gestión en Crisis.	Diaria
3.	**Activación (DESPUÉS)**	
3.1.	Definir los comunicados a ser liberados luego de declarar el evento como DESASTRE	00:15
3.2.	Efectuar las comunicaciones necesarias de acuerdo con el Plan de Gestión de Crisis	00:20
4.	**Operación en Contingencia (DESPUES)**	
4.1.	Definir las actividades a ser efectuadas para realizar el monitoreo de las personas interesadas e informar según corresponda.	00:30

4.2.	Efectuar las comunicaciones necesarias de acuerdo con el Plan de Gestión de Crisis, y mantener informado al Coordinador de Gestión en Crisis, la evolución de la situación.	Inmediato
5.	**Restauración (DESPUES)**	
5.1.	Definir las actividades a ser efectuadas para realizar el monitoreo de las personas interesadas e informar según corresponda.	N.A.
5.2.	Supervisión del mensaje emitido	00:20
6.	**Retorno o vuelta a la normalidad (DESPUES)**	
6.1.	Definir los comunicados a ser liberados para realizar el retorno a la normalidad.	N.A.
6.2.	Comunicar al personal, el estado de la situación actual y los detalles del retorno al centro de labores oficial o vuelta a la normalidad	N.A.
6.3.	Participar en sesión de labores aprendidas.	02:00

d. Rol: Voceros Nivel 3 (Medios de Comunicación)

Grupo:	**Equipo de Gestión en Crisis**	
Rol:	**Voceros Nivel 3**	
Nro	**Tarea, descripción**	**Frecuencia o Duración**
1.	**Actividades de Preparación (ANTES)**	
1.1.	Definir las actividades necesarias para tener los diferentes tipos de comunicado “listos” en caso ocurra un evento catalogado como DESASTRE	N.A.
1.2.	Participar en los simulacros de comunicación en crisis cuando se le es convocado.	01:00
2.	**Actividades de Respuesta (DURANTE)**	
2.1.	Definir las actividades necesarias para escalar el evento catalogado como ALERTA DE DESASTRE y luego de la evaluación correspondiente decidir si se declara el evento como DESASTRE	00:30
2.2.	Asistir a la convocatoria realizada por el Coordinador de Gestión en Crisis	Inmediato
2.3.	Dirigirse al área de acción que se le es asignada	00:20
2.4.	Participar en las personas dirigidas a los medios de comunicación, de acuerdo con el Plan de Gestión en Crisis.	Diaria
2.5.	Participar en las personas dirigidas a los Familiares de Personal Heridos o Muertos, de acuerdo con el Plan de Gestión en Crisis.	Diaria
3.	**Activación (DESPUÉS)**	
3.1.	Definir los comunicados a ser liberados luego de declarar el evento como DESASTRE	00:15
3.2.	Efectuar las comunicaciones necesarias de acuerdo con el Plan de Gestión de Crisis	00:20

4.	**Operación en Contingencia (DESPUES)**	
4.1.	Definir las actividades a ser efectuadas para realizar el monitoreo de las personas interesadas e informar según corresponda.	00:30
4.2.	Efectuar las comunicaciones necesarias de acuerdo con el Plan de Gestión de Crisis, y mantener informado al Coordinador de Gestión en Crisis, la evolución de la situación.	Inmediato
5.	**Restauración (DESPUES)**	
5.1.	Definir las actividades a ser efectuadas para realizar el monitoreo de las personas interesadas e informar según corresponda.	N.A.
5.2.	Supervisión del Mensaje Emitido	
6.	**Retorno o vuelta a la normalidad (DESPUES)**	
6.1.	Definir los comunicados a ser liberados para realizar el retorno a la normalidad.	N.A.
6.2.	Comunicar a su audiencia, el estado de la situación actual y los detalles del retorno al centro de labores oficial o vuelta a la normalidad	N.A.
6.3.	Participar en sesión de labores aprendidas.	02:00

3.5. Evaluación del Plan de gestión de la continuidad propuesto

Aplicando el método Delphi, se valoró el Plan de gestión de la continuidad propuesto. Los resultados de la valoración de las cuatro personas con responsabilidad y autoridad en el GRL en relación a la gestión de la continuidad de los procesos, se muestra a continuación:

				Jefatura de OFTI		Oficial de Seguridad de la Información		Jefe de Oficina RRHH		Jefe de la Oficina de Administración		TOTALES	
Variable	**Factor Relevante (indicador)**		**SI/NO**	**Peso (Madurez)**	**SI/NO**	**Peso (Madurez)**	**SI/NO**	**Peso (Madurez)**	**SI/NO**	**Peso (Madurez)**	**SI/NO**	**Peso (Madurez)**
	Análisis de impacto en el negocio (Business Impact Analysis-BIA)												
Business Impact Analysis (BIA)	1	¿Se ha realizado el análisis de procesos para identificar sus roles, funciones y activos críticos, con sus correspondientes valoraciones de criticidad y tiempos máximos de caída?	SI	**2**	SI	**2**	SI	**1**	SI	**2**	100%	**1.8**
	2	¿Se ha desarrollado el BIA, necesario para identificar y determinar los impactos operacionales, económicos y reputacionales, en la organización, en el caso de tener paralizaciones de los procesos?	SI	**1**	SI	**2**	SI	**1**	SI	**1**	100%	**1.3**
	3	¿Se ha identificado los recursos tecnológicos críticos para ser considerados en el Plan de gestión de la continuidad?	SI	**2**	SI	**3**	SI	**1**	SI	**2**	100%	**1.8**
		TOTAL (%)	100 %		100 %		100 %		100 %		100%	**1.6**
	Tolerancia de riesgo organizacional												
RTO y RPO	1	¿Se ha determinado las prioridades de recuperación de los procesos, identificando su Tiempo Objetivo de Recuperación (RTO) y su Punto Objetivo de Recuperación (RPO)?	SI	**2**	SI	**2**	SI	**1**	SI	**2**	100%	**1.8**

		TOTAL (%)	100 %		100 %		100 %		100 %		100%	**1.8**
	Evaluación de riesgos											
Identificación y priorización de activos	1	¿Se ha identificado y clasificado los activos de TI críticos que dan soporte a los procesos, para ser considerados en el análisis de riesgos de continuidad?	SI	**1**	SI	**2**	SI	**1**	SI	**2**	100%	**1.5**
	2	¿Se ha definido un criterio de priorización de los activos de TI y un procedimiento coherente para la valoración de su criticidad?	SI	**2**	SI	**2**	SI	**1**	SI	**2**	100%	**1.8**
Análisis de Amenazas	3	¿Se ha identificado las amenazas que pueden afectar a los activos de TI?	SI	**2**	SI	**2**	SI	**2**	SI	**2**	100%	**2.0**
	4	Se considera distintas clases de amenazas, como: ¿desastres naturales, desastres industriales, ataques intencionados, etc.?	SI	**2**	SI	**3**	SI	**3**	SI	**2**	100%	**2.5**
Análisis de Vulnerabilidades	5	¿Se ha realizado la identificación de vulnerabilidades existentes en el entorno de la organización, que podrían ser aprovechados por las amenazas para afectar a los activos de TI?	SI	**2**	SI	**2**	SI	**2**	SI	**2**	100%	**2.0**
Análisis de Escenarios de Riesgo	6	¿Se ha definido un criterio de valoración de los impactos de la caída de los activos de TI y su aplicación es suficiente y coherente?	SI	**1**	SI	**2**	SI	**1**	SI	**2**	100%	**1.5**
	7	¿Se ha definido un criterio de valoración de las probabilidades de ocurrencia de los escenarios de riesgo y su aplicación es suficiente y coherente?	SI	**1**	SI	**3**	SI	**2**	SI	**1**	100%	**1.8**
Evaluación de Riesgos	8	¿Se ha definido un sistema de valoración para determinar el nivel de exposición a los escenarios de riesgos?	SI	**1**	SI	**2**	SI	**2**	SI	**1**	100%	**1.5**
	9	¿Se ha valorado el nivel de exposición a los riesgos en base a información suficiente y pertinente?	SI	**2**	SI	**2**	SI	**3**	SI	**2**	100%	**2.3**

Escenarios de amenazas para la continuidad	10	¿Se han identificado los diferentes escenarios de paralización de los procesos críticos en base a los resultados de un análisis de riesgos?	SI	**2**	SI	**3**	SI	**2**	SI	**1**	100%	**2.0**
TOTAL (%)			100 %		100 %		100 %		100 %		100%	**1.9**
	Procedimientos de continuidad de negocio											
Diseño del plan de continuidad	1	¿Se han identificado las acciones actuales y se han definido las acciones preventivas para los diferentes escenarios de paralización de los procesos críticos?	SI	**1**	SI	**2**	SI	**3**	SI	**2**	100%	**2.0**
	2	¿Se han definido estrategias de continuidad y acciones de recuperación para los diferentes escenarios de paralización de los procesos críticos?	SI	**1**	SI	**2**	SI	**2**	SI	**2**	100%	**1.8**
TOTAL (%)			100 %		100 %		100 %		100 %		100%	**1.9**
	Soporte											
Roles, responsabilidades y autoridades organizacionales	1	¿Se ha definido una estructura organizativa de respuesta ante incidentes, con sus correspondientes roles y tiempos de actuación para llevar a cabo el Plan de continuidad?	SI	**2**	SI	**2**	SI	**2**	SI	**2**	100%	**2.0**
TOTAL (%)			100 %		100 %		100 %		100 %		100%	**2.0**

CONCLUSIONES

1. Se desarrolló un marco metodológico propio en 3 fases, basado en los marcos metodológicos de las normas ISO 22301 y la ISO 27001, mediante los cuales se desarrolló las fases principales de las actividades definiendo los procesos que serán considerados.
2. Del análisis de los procesos institucionales se identificó que los procesos Adquisición de bienes y servicios, Registro de nuevas adquisiciones margesí de bienes, Inventario de bienes, Registro y actualización de salida de bienes, Ingreso y salida de bienes de almacén, Percepción o recaudación de fondos, Elaboración de obligaciones presupuestarias, Ejecución financiera de la sede presidencial del GRL, Elaboración de planillas para personal, Control de asistencia y permanencia de personal, Elaboración de actividades y acciones de control y Defensa jurídica del GRL, son los procesos más críticos para el GRL y por consiguiente, deben estar considerados en el Plan de gestión de contingencias con el fin de mantener su disponibilidad por lo menos en sus funciones críticas. Para ello se lograron identificar los roles, funciones y activos tecnológicos críticos para cada caso.
3. Se realizó un análisis de impacto para cada proceso crítico, desde las perspectivas siguientes factores: financiero, afectación a usuarios internos, afectación a usuarios externos, afectación de la infraestructura, afectación a aspectos legales/contractuales, impacto a la imagen corporativa, impacto a la productividad de los trabajadores y afectación a la infraestructura física, identificándose que los procesos: Ejecución financiera de la sede presidencial del GRL, Elaboración de obligaciones presupuestarias y Percepción o recaudación de fondos son los procesos que generarían mayor impacto total para el GRL en caso de su interrupción parcial o total.
4. De la evaluación de los riesgos de cada activo tecnológico considerado como crítico con la se identificó que los escenarios de riesgo para los activos: Servidor principal de dominio, Servidor principal de base de datos y aplicaciones, Red de comunicaciones, son los que generan mayor exposición a los riesgos de continuidad; seguido de los activos Bases de Datos y Backups de base de datos.
5. Se identificaron las estrategias de contingencia actuales como Medidas actuales y preventivas; así como las estrategias correctivas o de recuperación para los siguientes escenarios de riesgo las acciones preventivas y correctivas para cada escenario de riesgo: Interrupción de la red, Interrupción del servicio eléctrico, Acciones malintencionadas, Fallas en los equipos terminales, Fallas en el software, Virus informáticos, Seguridad de personal, Robo de equipos e información. Adicionalmente, se consideró en esta actividad a los Desastres naturales/Industriales, por ser éste un escenario relacionada con la vida de las personas, por tanto, es un escenario crítico que se debe planificar su contingencia.

6. De los resultados de la validación del Plan de gestión de continuidad propuesto, a través del método Delphi, se concluye que tiene valoración entre los rangos de 1 a 2; y de acuerdo a la escala valorativa el Plan está aceptado como Clave y Relevante; lo que significa que la propuesta sirve a la OFTI para cumplir con su función de gestión de la continuidad y además que está desarrollada en concordancia con la norma ISO/IEC 22301, tomada como referencia.

RECOMENDACIÓN

1. Dado que la propuesta de Plan de gestión de la continuidad, solo barca la fase de operación que propone la norma ISO/IEC 22301, se recomienda continuar con otros estudios que agreguen procedimientos metodológicos para las demás etapas de planificación, evaluación y mejora.

REFERENCIAS BIBLIOGRÁFICAS

Alexander, A., & AMBCI. (2012). *Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012*. Recuperado el Agosto de 2019, de http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf

Avison, D., & Fitzgerald, G. (1995). *Information Systems Development: Methodologies, Techniques and Tools* (2da ed. ed.). Maidenhead, England: McGraw Hill.

Benavides, R. A. (2012). Curso a distancia sobre el gobierno de tecnologías de información y continuidad del negocio. México.

BSI GROUP. (2015). *Lineamientos para la implementación de las Normas ISO 9001 y ISO 22301 en las organizaciones.* Recuperado el Agosto de 2019, de Sitio Web oficial de BSI: http://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

Business Continuity Institute. (2018). BCI continuity and resilience report. Everbridge.

Carrillo, J. (2013). *Gestión del riesgo en las metodologías de proyectos de tecnologías de información y comunicaciones.* Recuperado el Agosto de 2019, de http://oaji.net/articles/2015/1783-1426290171.pdf

Centro de Coordinación de ITIL UTN FRBA. (s.f.). *Sobre ITIL: Centro de Coordinación de ITIL UTN FRBA*. Obtenido de Centro de Coordinación de ITIL UTN FRBA web site: http://www.cursositil.com.ar/index.php?option=com_content&view=article&id=44&Itemid=53

Chavarry Sandoval, C. J. (2012). *Propuesta de modelo ajustado a la gestión de TI/SI Orientado a los servicios basado en el marco de trabajo ITIL, caso de estudio aplicado al departamento de TI/SI de la Universidad de Lambayeque - Perú.* Chiclayo.

de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., & van Bon, J. (2008). *Estrategia del Servicio Basada en ITIL® V3 - Guía de Gestión.* Amersfoort, Holanda: Van Haren Publishing.

De la Cruz Ramírez, A., & Rosas Miguel, R. (2012). Implementación de un sistema service desk basado en ITIL. *Tesis*. México: Universidad Nacional Autónoma de México.

Dewar, W. R. (2011). Mejores Prácticas de Gestión. *Gerenc. Tecnol. Inform.* |, 11.

Ferrer, R. (2011). *Metodología para el diseño de un Plan de recuperación ante desastres O DRP.* Recuperado el Agosto de 2019, de http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_PLAN_RECUPERACION_ANTE_DESASTRES_DRP.pdf

Figuerola, N. (2008). Introducción a ITIL. *Serie Artículos sobre Gestión de IT y Calidad.*, pp. 2.

Gómez Alvarez, J. R. (2012). Implantación de los procesos de gestión de incidentes y gestión de problemas según ITIL v3.0 en el área de tecnologías de información de una entidad financiera. *Tesis*. Lima, Perú: Pontificia Universidad Católica del Perú.

González, J. (2015). Elaboración de un plan de auditoría para evaluación de cumplimiento en sistemas para gestión de la continuidad del negocio basado en la normativa ISO 22301. Costa Rica: Universidad de Costa Rica.

Harrington, H. (1992). *Mejoramiento de los procesos de la empresa.* Bogotá: McGraw-Hill.

INDECOPI. (2008). NTP-ISO/IEC 27001. EDI. . Tecnología de la Informacion.Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. *Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual*. Obtenido de Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

ISACA. (2009). Guía del usuario de COBIT para Gerentes de Servicios. 1.

Lozano Sandova, F., & Rodríguez Mejía, K. (2011). Modelo para la implementación de ITIL en una institución universitaria. *Tesis.* Santiago de Cali: Universidad ICESI.

Lucio Nieto, T. d. (2013). *Marco para la definición y adecuación de una service management office en el contexto de los servicios de tecnologías de la información.* Legenés.

Magerit. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Ministerio de Hacienda y Administraciones Públicas de España.

Martinez, J. (2016). El plan de continuidad de negocio. España: Diaz de Santos.

Medina Cárdenas, Y. C., & Rico Bautista, D. W. (2011). Mejores Prácticas de Gestión. 11.

OSI. (2010). *Seguridad de la Sociedad: Sistemas de Continuidad del Negocio – Requisitos.* Obtenido de International Organization for Standardization: https://www.pea.co.th/BCM/DocLib/ISO_22301_2012.pdf

Ramírez, T., Calderas, R., & Benavides, A. (2012). Curso a distancia sobre el gobierno de tecnologías de información y continuidad del negocio. México.

Ruiz Carreira, M., & Toro Bonilla, M. (2010). *Simulación aplicada a la mejora de los procesos de gestión de servicios ti.* Cadíz, España.

Salgueiro, A. (2004). *Como mejorar los procesos y la productividad.* (A. E. Certificación, Ed.) Madrid, España: AENOR.

Sandhusen, R. (2002). *Mercadotecnia* (ISBN 9789702402473 ed.). CECSA (Compañía Editorial CONTINEN).

SISTESEG. (2016). *Business Impact Analysis.* Recuperado el Junio de 2019, de http://www.sisteseg.com/files/Microsoft_Word_-_BIA_BUSINESS_IMPACT_ANALYSIS.pdf

Spiñeira, Sheldon y Asociados. (2015). *Desarrollo de un plan de continuidad del Negocio: Aplicando un enfoque rápido, económica y efectivo.* Recuperado el julio de 2019, de https://www.pwc.com/ve/es/asesoriagerencial/boletin/assets/boletin-advisory-edicion-09-2008.pdf

Stanton, W. J., Etzel, M. J., & Walker, B. J. (2007). *Fundamentos de Marketing* (14 ava edición ed.). Mexico DF, Mexico: McGraw-Hill / Interamericana Editores, S.A.

Thejendra, B. (2014). *thejendra.com*. Recuperado el 2014, de thejendra.com: http://www.thejendra.com/ARTICLES/ITIL.htm

Trischler, W. (2008). *Mejora del valor añadido en los procesos.* Ediciones Gestión 2000.

Ureña, M. (2011). *Sistema de Gestión de Continuidad del Negocio de acuerdo con BS 25999 e ISO 22301*. Recuperado el Agosto de 2019, de http://sasorigin.onstreammedia.com/origin/isaca/LatinCACS/cacslat/forSystemUse/papers/133.pdf

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (. (2008 b). *Diseño del Servicio Basada en ITIL® V3 - Guía de Gestión* (Primera edición ed.). Zaltbommel, Holanda: Van Haren Publishing.

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (2008 a). *Estrategia del servicio basada en ITIL v3 - Guia de Gestión* (1 era edición ed.). Amersfoort, Holanda: Van Haren Publishing.

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (2008 d). *Operación del Servicio Basada en ITIL® V3 - Guía de Gestión* (Primera edición ed.). Zaltbommel, Holanda: Van Haren Publishing.

Vásquez O., A. (2014). Uso del ciclo de vida de ITIL para la adopción de servicios en la nube para PYMES mexicanas. *Tesis de maestría en administración de servicios de tecnologías de la información*. México: Universidad Iberoamericana.

ANEXOS

ANEXO N° 1: Formato para la Evaluación del cumplimiento de la seguridad de la información el en GRL

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
ESCUELA DE POSTGRADO

MAESTRIA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DE SOFTWARE

Tesis: Plan de Gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque

EVALUACIÓN DEL CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Control ISO	Requerimiento Objetivo de control	Control que debe evidenciarse	Existe? o Está implementado?	Sustente Cómo o Por qué?
5. Política de seguridad				
5.1	**Política de Seguridad de la Información**			
5.1.1	Se tiene documento de la política de seguridad de la Información	Un documento de política de seguridad de la información debería ser aprobado por la Dirección y debería ser publicado y comunicado a todos los empleados y terceras partes.		
5.1.2	Se hace revisión y evaluación de este documento y se promulga su lectura y aplicación.	La política de seguridad de la información se debería revisar a intervalos planificados o en el caso de que se produzcan cambios significativos para asegurar la idoneidad, adecuación y la eficiencia de la continuidad.		
6. Organización de la Seguridad de la Información				
6.1	**Organización Interna**			

6.1.1	Compromiso de las Dirección con la seguridad de la información	La Dirección deberá dar un activo soporte a la seguridad dentro de la organización a través de directivas claras, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de seguridad de la información.		
6.1.2	Coordinación de la Seguridad de la Información	Las actividades relativas a la seguridad de la información deberían ser coordinadas por representantes de las diferentes partes de la organización con los correspondientes roles y funciones de trabajo.		
6.1.3	Asignación de responsabilidades sobre la seguridad de la información	Debería definirse claramente todas las responsabilidades de seguridad de la información.		
6.1.4	Proceso de Autorización de recursos para el procesamiento/tratamiento de información	Debería definirse e implantarse un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información.		
6.1.5	Acuerdos de confidencialidad	Debería identificarse y revisarse de una manera regular los requisitos de los acuerdos de confidencialidad o no revelación que refleje las necesidades de la organización para la protección de la información.		
6.1.8	Se realiza Auditoría interna - Revisiones independientes de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación debería revisarse de una manera independiente a intervalos planificados o cuando se producen cambios significativos en la implantación de la seguridad.		
6.2	**Seguridad de acceso de terceras partes**			

6.2.1	Identificación de riesgos de acceso de terceras partes	Cuando el negocio requiera de partes externas, deberían identificarse los riesgos de la información de la organización y de los dispositivos de tratamiento de la información, así como la implantación de los controles adecuados antes de garantizar el acceso.		
6.2.2	Consideraciones de seguridad en contratos con clientes	Todos los requisitos de seguridad que se hayan identificado deberían ser dirigidos antes de dar acceso a los clientes a los activos o a la información de la seguridad.		
6.2.3	Consideraciones de seguridad en contratos con terceros	Los acuerdos que comparten el acceso de terceros a recurso de tratamiento de información de la organización deben basarse en un contrato formal que tenga o se refiera a todos los requisitos de la seguridad que cumpla con las políticas y normas de seguridad de la organización. El contrato debe asegurar que no hay malentendidos entre la organización y los terceros. Las organizaciones deben verse compensadas hasta la indemnización de sus suministradores.		
7. Gestión de activos				
7.1	**Responsabilidad sobre los activos**			
7.1.1	Inventario de activos tecnológicos y de la información.	Todos los activos deberían ser claramente identificados y deberían prepararse y mantenerse un inventario de todos los activos importantes.		
7.1.2	Responsables/Propietarios de los activos tecnológicos	Toda la información y los activos asociados con los recursos para el tratamiento de la información deberían ser propiedad de una parte designada de la organización.		

7.1.3	Uso aceptable de las activos tecnológicos	Las reglas de uso aceptable de la información y los activos asociados con el tratamiento de la información, deberían ser identificadas, documentadas e implantadas.		
7.2	**Clasificación de la información**			
7.2.1	Normas y directrices para clasificación de la información	La información debería estar clasificada, según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.		
7.2.2	Identificación, etiquetado y manejo de la información	Debería desarrollarse un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización.		
8. Seguridad ligada a los Recursos Humanos				
8.1	**Seguridad en actividades previas en la contratación**			
8.1.3	Términos y condiciones laborales	Como parte de las obligaciones contractuales, los empleados, contratistas y usuarios de tercera parte deberían aceptar y firmar los términos y condiciones de su contrato de trabajo, que deberían establecer sus responsabilidades, así como las de la organización en lo relativo a la seguridad de la información.		
8.2	**Seguridad en actividades durante el desempeño de las funciones**			
8.2.1	Responsabilidades de la Dirección	La Dirección debería requerir a los empleados, contratistas y de tercera parte, el aplicar la seguridad de acuerdo a lo establecido en las políticas y procedimientos de la organización.		

8.2.2	Conciencia y formación sobe la seguridad de la información: educación y entrenamiento	Todos los empleados de la organización y, cuando corresponda, los contratistas y los usuarios de tercera parte, deberían recibir una formación y concientización adecuadas y actualizadas de las políticas y procedimientos, según corresponda a su puesto de trabajo.		
8.2.3	Procesos disciplinarios	Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna brecha de seguridad.		
8.3	**Fin de contrato o cambio de funciones**			
8.3.1	Responsabilidades en la terminación del contrato	Las responsabilidades para llevar a cabo la finalización o cambio de puesto de trabajo deberían estar claramente definidas y asignadas.		
8.3.2	Devolución/restitución de activos tecnológicos	Todos los empleados, contratistas y usuarios de tercera parte deberían devolver los activos de la organización que tengan en posesión a la finalización de su empleo, contrato o acuerdo.		
8.3.3	Eliminación de permisos sobre los activos	Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y usuarios de tercera parte, debería ser retirada a la finalización de la contratación o del acuerdo, o adaptados según los cambios.		
9. Seguridad física y del entorno				
9.1	**Áreas seguras/restringidas**			

9.1.1	Perímetro de Seguridad Física	Debería usarse perímetros de seguridad (barreras tales como muros, puertas de entrada con control a través de tarjeta o mesas de recepción tripuladas) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.		
9.1.2	Controles físicos de entrada	Las áreas seguras deberías estar protegidas por controles de entrada adecuados para asegurar que únicamente se permita el acceso al personal autorizado.		
9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	Se debería diseñar y aplicar la seguridad física para las oficinas, despachos y recursos.		
9.1.4	Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar una protección física contra el daño por fuego, inundación, terremoto, explosión, malestar social y otras formas de desastres naturales o provocadas por el hombre.		
9.1.5	Trabajo en áreas restringidas	Se debería diseñar e implantar la protección física y las directrices para trabajar en las áreas seguras.		
9.2	**Seguridad de los equipos**			
9.2.1	Ubicación, instalación y protección de equipos tecnológicos	Los equipos deberías estar situados o protegidos para reducir los riesgos de las amenazas y los riesgos del entorno, así como de las oportunidades de acceso no autorizado.		
9.2.2	Seguridad en el suministro de electricidad y servicios (utilities)	Los equipos deberías estar protegidos de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.		

9.2.3	Seguridad en el cableado	El cableado eléctrico y de telecomunicaciones que transmiten datos a los servicios de soporte de la información debería estar protegido de interceptación o de daños.		
9.2.4	Mantenimiento de equipos	Los equipos deberías ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.		
9.2.5	Seguridad de equipos fuera de las áreas seguras	Se debería aplicar medidas de seguridad a los equipos fuera de los locales de la organización, teniéndose en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización.		
9.2.6	Destrucción y reutilización de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deberían ser comprobados para asegurar que todo dato sensible y software bajo licencia se ha borrado o sobrescrito, previamente a su utilización.		
9.2.7	Traslado de activos fuera de la organización	Los equipos, la información o el software no deberían sacarse fuera de las instalaciones sin previa autorización.		
10. Gestión de las comunicaciones y las operaciones				
10.1	**Procedimientos y responsabilidades operativas**			
10.1.1	Documentación de procesos operativos	Se debería implantar, mantener procedimientos operacionales y estar disponibles para todos los usuarios que lo necesiten.		

10.1.2	Control de Cambios	Se deberían controlar los cambios en los recursos y sistemas de tratamiento de la información.		
10.1.3	Segregación de funciones y tareas	Las tareas y áreas de responsabilidad deberían segregarse para reducir la posibilidad de modificaciones no autorizadas y no intencionadas o el mal uso de los activos de la organización.		
10.1.4	Separación de los ambientes de Desarrollo, prueba y producción	Deberían separarse los recursos para el desarrollo, las pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema operativo.		
10.2	**Gestión de la provisión de servicios contratados con terceros**			
10.2.1	Entrega de servicios	Deberían asegurarse de que los controles de seguridad, los niveles de entrega y definiciones del servicio incluido en el acuerdo de entrega del servicio por tercera parte se implantan, se ponen en funcionamiento y son mantenidos por la tercera parte.		
10.2.2	Monitoreo y revisión de servicios de terceros	Los servicios, informes y registros proporcionados por las terceras partes deberían ser controlados y revisados regularmente, y también se deberían llevar a cabo auditorías regularmente.		
10.2.3	Administración de cambios a servicios de terceros	Se deberían gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio implicados y la revalorización de los riesgos.		
10.4	**Protección contra software malicioso y código móvil**			

10.4.1	Controles contra código malicioso	Se debería implantar procedimientos de concienciación del usuario adecuados; así como controles de detección, prevención y recuperación para proteger contra código malicioso.		
10.4.2	Controles contra código móvil	Cuando se autoriza el uso de código ambulante, la configuración debería asegurar que está operando un código ambulante autorizado de acuerdo a una política de seguridad claramente definida, y debería prevenirse la ejecución de código ambulante no autorizado.		
10.5	**Copias de seguridad**			
10.5.1	Copias de respaldo de la información.	Se debería hacer copias de seguridad de la información y del software y ser comprobadas regularmente de acuerdo con la política de copias de seguridad acordadas.		
10.6	**Gestión de la seguridad de red**			
10.6.1	Controles de la Red	Las redes deberían estar adecuadamente gestionadas y controladas, para estar protegidas de amenazas y para mantener la seguridad de los sistemas y aplicaciones que usan estas redes, incluyendo la información en tránsito.		
10.6.2	Seguridad de los Servicios de Red	Las características de seguridad, los niveles de servicio, los requisitos de gestión para todos los servicios de red deberían estar identificadas e incluidas en todo acuerdo de servicio de red, aunque estos servicios se proporcionen desde dentro de la organización o sean subcontratados.		

10.7	**Utilización de los soportes de información**			
10.7.1	Administración de medios removibles	Debería haber procedimientos para la gestión de los soportes desmontables.		
10.7.2	Destrucción de medios	Debería deshacerse de los soportes de una manera segura y fuera de peligro cuando no se vaya a requerir su uso durante más tiempo, mediante procedimientos formales.		
10.7.3	Procedimientos de manejo de la información	Se debería establecer procedimientos para el tratamiento y el almacenamiento de la información para proteger esta información de revelación no autorizada o mal uso.		
10.7.4	Seguridad de la documentación de los sistemas	El sistema de documentación debería estar protegido contra accesos no autorizados.		
10.8	**Intercambio de información**			
10.8.1	Políticas y procedimientos del intercambio de información	Se debería establecer políticas de intercambio formal, procedimientos y controles para proteger el intercambio de la información mediante el uso de todos los tipos de servicios de comunicación.		
10.8.2	Acuerdos para el intercambio de información.	Se debería establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.		
10.8.3	Medios físicos en movimiento	Los recursos que contienen información deberían estar protegidos contra el acceso no autorizado, el mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.		

10.8.4	Mensajería electrónica	La información implicada en el envío de mensajes electrónicos debería estar adecuadamente protegida.		
10.8.5	Sistemas de información de negocios	Se debería desarrollar e implantar políticas y procedimientos para proteger la información asociada a la interconexión de sistemas de información entre organizaciones.		
11. Control de accesos				
11.1	**Requerimientos de negocio para control de acceso**			
11.1.1	Política de Control de Acceso	Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad para el acceso.		
11.2	**Gestión de acceso de los usuarios**			
11.2.1	Registro de usuarios	Debería haber un procedimiento de registro formal de usuarios y de retirada del registro para conceder y revocar el acceso a todos los sistemas y servicios de información.		
11.2.2	Administración de privilegios	La asignación y el uso de privilegios debería estar restringidos y controlados.		
11.2.3	Administración de contraseñas de usuario (passwords)	La asignación de contraseñas debería ser controlada a través de un proceso formal de gestión.		
11.2.4	Revisión de los permisos asignados a los usuarios	La Dirección debería revisar los derechos de acceso de los usuarios a intervalos regulares y utilizando un procedimiento formal.		
11.3	**Responsabilidad de los usuarios**			

11.3.1	Uso de las contraseñas	Se debería requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de contraseñas.		
11.3.2	Equipos desatendidos	Los usuarios deberían asegurarse que el equipo desatendido tiene la protección adecuada.		
11.3.3	Política de escritorios y pantallas limpias	Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.		
11.4	**Control de acceso a la red**			
11.4.1	Políticas para el uso de los servicios de la red de datos	Únicamente se debería proporcionar a los usuarios el acceso a los servicios para los que específicamente se les haya autorizado el uso.		
11.4.2	Autenticación de usuarios para conexiones externas	Se debería utilizar los métodos apropiados de autenticación para el control de acceso a los usuarios en remoto.		
11.4.3	Identificación de equipos en la red	Debería considerarse la identificación automática del equipo como un medio de autenticación de las conexiones para las posiciones y equipos específicos.		
11.4.4	Diagnóstico remoto y protección de la configuración de puertos	Se debería controlar acceso físico y lógico al diagnóstico y configuración de los puertos.		
11.4.5	Segregación en la red	Los grupos de servicio de información, de usuarios y de sistema de información deberían estar segregados en redes.		

11.4.6	Control de conexión a la red	Se debería restringir la capacidad de los usuarios a conectarse a la red en el caso de redes compartidas, especialmente para aquellas que traspasan las fronteras de la organización, en línea con la política de control de acceso y los requisitos de las aplicaciones de negocio.		
11.4.7	Control de enrutamiento de la red	Los controles de direccionamiento deberían estar implantados para las redes, para asegurar que las conexiones de las computadoras y los flujos de información no violen la política de control de acceso a las aplicaciones del negocio.		
11.5	**Control de acceso a los sistemas operativos**			
11.5.1	Procedimientos para inicio de sesión de las estaciones de trabajo	Se debería controlar el acceso al sistema operativo mediante un procedimiento de entrada seguro.		
11.5.2	Identificación y autenticación de los usuarios.	Todos los usuarios deberían tener un identificador de usuario (ID) para su uso personal y único. Se debería elegir una técnica adecuada de autenticación para la conformación de la identidad de un usuario.		
11.5.3	Sistema de administración de contraseñas.	Los sistemas para la administración de contraseñas deberían ser interactivos y asegurar la calidad de la contraseña.		
11.5.4	Uso de las utilidades del sistema	El uso de los programas que pueden ser capaces de invalidar los controles del sistema y de la aplicación, deberían estar restringidos y estrictamente controlados.		
11.5.5	Desconexión automática de sesión.	Las sesiones interactivas deberían cerrase después de un periodo de inactividad definido.		

11.5.6	Limitación en los periodos de tiempo de conexión a servicios y aplicaciones	Se debería usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.		
11.6	**Control de acceso a la información y aplicaciones**			
11.6.1	Restricción de acceso a los sistemas de información	Debería restringirse el acceso de los usuarios y del personal de apoyo a la información y a las funciones del sistema de aplicación, de acuerdo con la política de control de acceso definida.		
11.6.2	Aislamiento de sistemas sensibles	Los sistemas sensibles deberían tener un entorno de computadores dedicados y aislados.		
11.7	**Computación móvil y teletrabajo**			
11.7.1	Computación y comunicaciones móviles	Debería implantarse una política formal y debería adoptarse las apropiadas medidas de seguridad para proteger contra los riesgos de la utilización de computadores y comunicaciones móviles.		
11.7.2	Teletrabajo	Se deberían desarrollar e implantar procedimientos, planes operacionales y una política para las actividades de teletrabajo.		
12. Adquisición, desarrollo y mantenimiento de sistemas de información				
12.1	**Requisitos de seguridad de los sistemas de información**			
12.1.1	Análisis y especificaciones de los requerimientos de seguridad			
12.5	**Seguridad en los procesos de desarrollo y soporte**			

12.5.1	Procedimientos para el control de cambios	La implementación de cambios debería estar controlada mediante el uso de procedimientos formales de control de cambios.		
12.5.2	Revisión técnica de aplicaciones después de cambios al sistema operativo	Cuando se realizan cambios en los sistemas debería revisarse y probarse las aplicaciones, sobre todas las críticas, para garantizar que no existen efectos adversos en las operaciones organizativas o la seguridad.		
12.5.3	Restricciones a cambios en paquetes de software	No debería estimularse las modificaciones a los paquetes de software, debería limitarse a los cambios necesarios y todos los cambios deberían estar estrictamente controlados.		
12.5.4	Fuga de información	Debería evitarse la oportunidad de fuga de información.		
12.5.5	Desarrollo de software por parte de Outsourcing	La externalización del desarrollo del software debería ser supervisada y monitorizada por la organización.		
12.6	**Gestión de vulnerabilidades técnicas**			
12.6.1	Control de vulnerabilidades técnicas	Debería obtenerse información oportuna a cerca de las vulnerabilidades técnicas de los sistemas de información que se estén utilizando. Asimismo, deberían evaluarse la exposición de la organización a dichas vulnerabilidades y deberían adoptarse medidas adecuadas para afrontar el riesgo asociado.		
13. Gestión de incidentes de seguridad de la información				
13.1	**Comunicación de eventos y debilidades de seguridad de la información**			
13.1.1	Reporte de eventos de Seguridad de la información.	Los eventos de seguridad de la información deberían comunicarse mediante canales adecuados de gestión lo antes posible.		

13.1.2	Reporte de debilidades de seguridad	Todos los trabajadores, contratistas y usuarios terceros de los sistemas y servicios de comunicación deberían estar obligados a anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios.		
13.2	**Gestión de incidentes de seguridad de la información y de su mejoramiento**			
13.2.1	Responsabilidades y procedimientos	Debería establecerse responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.		
13.2.2	Aprendizaje a partir de los incidentes de seguridad	Deberían existir mecanismos para permitir que los tipos, volúmenes y costes de los incidentes de seguridad de la información se cuantifiquen y se supervisen.		
13.2.3	Recolección de evidencia	Cuando una acción contra una persona u organización después de un incidente de seguridad de la información implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas establecidas en la jurisdicción pertinente con respecto a las pruebas.		
14. Gestión de la continuidad del negocio				
14.1	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**			
14.1.1	Inclusión de seguridad de la información en el proceso de administración de la continuidad del negocio	Debería desarrollarse y mantenerse un proceso controlado para la continuidad del negocio en toda la organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.		

14.1.2	Continuidad del negocio y análisis de impacto (BIA)	Deberían identificarse los eventos que provocan interrupciones en los procesos del negocio; así como la probabilidad y los efectos de dichas interrupciones y sus consecuencias con respecto a la seguridad de la información.		
14.1.3	Desarrollo e implementación de planes de continuidad	Debería desarrollarse e implantarse planes para mantener o restaurar las actividades y garantizar la disponibilidad de la información en el nivel y la escala temporal requeridos después de una interrupción o un fallo de los procesos críticos de un negocio.		
14.1.4	Marco de planeación para la continuidad del negocio	Se debería mantener un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, para dirigir de una manera coherente los requisitos de seguridad de la información, y para identificar prioridades para las pruebas y el mantenimiento.		
14.1.5	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio	Los planes de continuidad del negocio deberían probarse y actualizarse periódicamente para garantizar que están al día y que son efectivos.		
15. Conformidad				
15.1	**Cumplimiento con requerimientos legales**			
15.1.1	Identificación de la legislación aplicable	Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse explícitamente, documentarse y mantenerse actualizados para cada sistema de información y la organización.		

15.1.2	Derechos de autor y propiedad intelectual	Deberían implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales acerca del uso de materiales con respecto a los cuales puedan existir derechos de propiedad intelectual y acerca del uso de productos de software exclusivo.		
15.1.3	Salvaguardar los registros de la organización	Los registros importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios contractuales y empresariales.		
15.1.4	Protección de los datos y privacidad de la información personal	Debería garantizarse la protección de datos y la privacidad según se requiera en la legislación, las normativas y, si fuera aplicable, las cláusulas contractuales pertinentes.		
15.1.5	Prevención del mal uso de los componentes tecnológicos	Debería impedirse que los usuarios utilizaran las instalaciones de procesamiento de la información para fines no autorizados.		
15.1.6	Regulación de controles criptográficos	Los controles criptográficos deberían utilizarse de acuerdo con todos los contratos, leyes y normativas pertinentes.		
15.2	**Conformidad con políticas y normas de seguridad y conformidad técnica**			
15.2.1	Cumplimiento de los diferentes requerimientos y controles establecidos por la política de seguridad	Los gestores deberían asegurarse de que todos los procedimientos de seguridad, dentro de su área de responsabilidad, se realicen con el fin de cumplir las políticas y normas de seguridad.		
15.2.2	Chequeo del cumplimiento técnico	Debería comprobarse periódicamente que los sistemas de información cumplan las normas de implementación de seguridad.		

15.3	**Consideraciones sobre la auditoría de sistemas de información**			
15.3.1	Controles para auditoría del sistema	Los requisitos y actividades de la auditoría que impliquen comprobaciones en los sistemas operativos, deberían planificarse cuidadosamente y acordarse, para minimizar los riesgos de interrupciones de los procesos.		
15.3.2	Protección de las herramientas para auditoría del sistema	El acceso a las herramientas de auditoría de los sistemas de información debería estar protegidos para evitar cualquier posible peligro o uso indebido.		

ANEXO N° 2: Formato para el análisis de riesgos operativos de TI

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
ESCUELA DE POSTGRADO

MAESTRIA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DE SOFTWARE

Tesis: Plan de Gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque

ANÁLISIS DE RIESGOS OPERATIVOS DE TI

En el siguiente formato contiene el resumen del análisis y evaluación de los posibles riesgos relacionados con Tecnología de la Información que afectan directamente los activos tecnológicos.

I. SERVIDORES Y CONCENTRADORES CENTRALES

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Acceso no autorizado		
Corte de luz, Sistema ininterrumpido de energía (UPS) descargado o variaciones de voltaje		
Destrucción o fallo de un componente crítico del equipo (microprocesador, memoria, fuente de poder, otros)		
Errores de configuración		
Factores ambientales no adecuados. (ventilación, protección contra incendios, acondicionamiento racks, otros)		
Límite de vida útil – Máquinas obsoletas (antigüedad del equipo, repotenciamiento de componentes)		
Mantenimiento		
Robo		
Afectación por virus		

II. BASE DE DATOS

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Copia no autorizada de o a un medio de datos externos		
Errores de software (motor y contenedor de base de datos)		
Falta de espacio de almacenamiento		
Pérdida o falla de backups		
Pérdida de confidencialidad en datos privados y de sistema		
Directorios compartidos		
Sabotaje		
Afectación de virus		

III. SOFTWARE BACKOFFICE Y SISTEMAS OPERATIVOS

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Aplicaciones sin licencias		
Error de configuración		
Mala Administración de control de accesos		
Pérdida de datos		
Afectación de virus		

IV. BACKUP (SISTEMA DE RESPALDO)

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Copia no autorizada del backup		
Errores de software para recuperación de información de backup (restore)		
Falla o deterioro del medio de almacenamiento externo del backup		
Falta de espacio de almacenamiento		
Mala integridad de los datos resguardados al recuperar la información de un backup		
Medios de datos no están disponibles cuando son necesarios		
Pérdida o robo de backups		
Sabotaje		

V. CABLEADO Y CONCENTRADORES

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Conexión de cables inadmisible (modificación de conexiones y mal etiquetado)		
Daño o destrucción, de cables o equipamiento, inadvertido (mala ubicación, por limpieza, impedimento de libre tránsito, otros)		
Factores ambientales		
Accesos no autorizados.		
Longitud de los cables de red excedidos a las normas		

VI. RED

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)		
Configuración inadecuada de componentes de red		
Errores de operación (mala estandarización de velocidades de transmisión y ancho de banda, otros)		
Mal uso de servicios de red		

VII. USUARIOS

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Acceso no autorizado a datos		
Borrado, modificación o revelación de claves de acceso a la información y aplicaciones, desautorizada o inadvertida		
Condiciones de trabajo adversas (ergonomía, ubicación de equipos, otros)		
Destrucción negligente de datos por parte de los usuarios		
Documentación deficiente (manual de usuario)		
Entrada sin autorización a ambientes		
Entrenamiento de usuarios inadecuado		
Falta de controles y log de las transacciones realizadas por los usuarios.		
No cumplimiento con las medidas de seguridad del sistema		
Desvinculación del personal con la institución		

VIII. DOCUMENTACIÓN DE LOS SISTEMAS EN PRODUCCIÓN

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Acceso no autorizado a datos de documentación		
Borrado, modificación o revelación desautorizada de información		
Copia no autorizada de un medio de documentación del sistema		
Descripción de archivos y programas inadecuado		
Documentación insuficiente o faltante, en relación a seguridad de la información		
Mantenimiento y actualización inadecuado o ausente de la documentación		

X. SISTEMAS O APLICACIONES INFORMÁTICAS EN PRODUCCIÓN

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Inadecuada gestión de cambios		
Funcionalidad del sistema (no atiende todos los requerimientos de los usuarios y áreas)		
Acceso a los programas fuentes no controlado		
Validación en los procesos de captura y registro de transacciones		
Sabotaje (eliminación de programas)		

ANEXO N° 3: Formato para la Evaluación del Plan de Gestión de la continuidad del negocio actual del GRL

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
ESCUELA DE POSTGRADO

MAESTRIA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DE SOFTWARE

Tesis: Plan de Gestión de la continuidad de negocio basado en la norma ISO 22301 para la Oficina de Tecnologías de la Información del Gobierno Regional de Lambayeque

CARGO / NIVEL: _____

IMPORTANTE: CONTESTAR TODAS LAS PREGUNTAS, DEJAR UNA DE ELLAS SIN CONTESTAR INVALIDA LA ENCUESTA

PREGUNTA	NIVEL DE INTESIDAD
1. ¿La Gestión Estratégica de TI incluye la planeación de la continuidad del negocio basada en la identificación y análisis de riesgos?	Nada 1 | 2 | 3 | 4 | Mucho 5
2. ¿La etapa de planificación de las actividades de TI, antes de su ejecución, contribuye al mejoramiento continuo de la organización?	Nunca 1 | 2 | 3 | 4 | Siempre 5
3. ¿La calidad de los desarrollos realizados en el Área de TI realizadas contribuye a la productividad y competitividad de la organización?	Nada 1 | 2 | 3 | 4 | Mucho 5
4. ¿La organización cuenta con un Plan de Continuidad del Negocio y está estructurado para responder oportunamente ante un evento inesperado?	Nada 1 | 2 | 3 | 4 | Mucho 5
5. ¿Se implementan ejercicios de Respuesta y Recuperación ante la posible ocurrencia de un evento inesperado y se cuenta con los recursos necesarios?	Nada 1 | 2 | 3 | 4 | Mucho 5
6. ¿Se realiza la identificación y análisis de riesgos como parte del Análisis del Impacto del Negocio?	Nunca 1 | 2 | 3 | 4 | Siempre 5
7. ¿La organización está expuesta a riesgos internos y externos que la hacen vulnerable a pérdidas operativas, financieras y reputacionales?	Nunca 1 | 2 | 3 | 4 | Siempre 5
8. ¿Se reconoce la magnitud de los impactos generados por una interrupción de los servicios en caso de materializarse un riesgo?	Nada 1 | 2 | 3 | 4 | Mucho 5

9. ¿Se han determinado tiempos de recuperación cuando los sistemas dejan de funcionar ante un evento inesperado?	Nada 1	2	3	4	Mucho 5
10. ¿Se elabora y desarrollo un Plan de Pruebas de los controles y procedimientos para demostrar su efectividad?	Nunca 1	2	3	4	Siempre 5
11. Sobre los controles instalados en su equipo y sistemas, ¿considera usted que le han ayudado a mitigar los riesgos?	Nada 1	2	3	4	Mucho 5
12. ¿Se han conformado Comisiones Especiales, con funciones específicas para activarse y actuar en caso de emergencias e incidencias que pueden paralizar los procesos o afectar la salud de las personas?	Nunca 1	2	3	4	Siempre 5
13. ¿Siente que la capacitación o entrenamiento que ha recibido en relación a las políticas de seguridad de la información le ha ayudado para resolver cualquier problema o incidente que se ha presentado?	Nada 1	2	3	4	Mucho 5
14. Considerando a su organización ¿Tiene usted la voluntad de hacer el mayor esfuerzo, más allá de lo normalmente esperado, para cumplir y usar adecuadamente las políticas de seguridad de la información?	Poca 1	2	3	4	Mucha 5
15. En caso que ocurra alguna incidencia, ¿sabe cómo actuar según las políticas de seguridad de la información de la institución donde labora?	Nunca 1	2	3	4	Siempre 5
16. Por el buen desempeño de sus labores en relación al cumplimiento de las políticas de seguridad, ¿están claramente establecidos los reconocimientos en la organización?	Nunca 1	2	3	4	Siempre 5
17. Se dice que en su trabajo "se trabaja bajo objetivos y presión". ¿Considera usted que puede lograrse un trabajo sin errores bajo estas condiciones?	Nunca se logra 1	2	3	4	Siempre se logra 5
18. En su trabajo, ¿con qué frecuencia a cometido errores de seguridad de información (registro de datos, errores de cálculo, etc.) debido a la presión y carga de trabajo?	Poca 1	2	3	4	Mucha 5
19. Considera que la empresa ha implementado políticas para el manejo del tiempo y carga de trabajo han logrado su objetivo	Poco 1	2	3	4	Mucho 5
20. Cuántos errores relacionados con sistemas de información usted ha cometido por falta de conocimiento de las políticas de seguridad de la información.	Pocos 1	2	3	4	Muchos 5

ANEXO N° 4: Tablas de referencia para la valoración de la criticidad de los activos de TI

Para la valoración de los activos se tomarán en cuenta las siguientes dimensiones de seguridad:

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Fuente: (Magerit, 2012)

[pi] Información de carácter personal	
10	probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
9	probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7 – 8	probablemente afecte a un grupo de individuos y probablemente quebrante leyes o regulaciones
5 – 6	probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación
3 – 4	pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones
1 – 2	pudiera causar molestias a un individuo
[lpo] Obligaciones legales	
9 - 10	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7 - 8	probablemente cause un incumplimiento grave de una ley o regulación
5 - 6	probablemente sea causa de incumplimiento de una ley o regulación
3 – 4	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1 – 2	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad	
9 - 10	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
7 - 8	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
5 - 6	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3 – 4	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1 – 2	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales económicos	
9 - 10	de enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7 - 8	de alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

5 - 6	de cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3 – 4	de bajo interés para la competencia de bajo valor comercial
1 – 2	de pequeño interés para la competencia de pequeño valor comercial supondría pérdidas económicas mínimas
[da] de interrupción del servicio	
9 - 10	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones Probablemente tenga un serio impacto en otras organizaciones
7 - 8	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5 - 6	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones
3 – 4	Probablemente cause la interrupción de actividades propias de la Organización
1 – 2	Pudiera causar la interrupción de actividades propias de la Organización
[po] de orden público	
9 - 10	alteración seria del orden público
7 - 8	probablemente cause manifestaciones, o presiones significativas
3 - 6	causa de protestas puntuales
1 – 2	pudiera causar protestas puntuales
[op] operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7 – 8	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5 – 6	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3 – 4	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1 – 2	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] administración y gestión	
9 - 10	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7 - 8	probablemente impediría la operación efectiva de la Organización
5 - 6	probablemente impediría la operación efectiva de más de una parte de la Organización
3 – 4	probablemente impediría la operación efectiva de una parte de la Organización
1 – 2	pudiera impedir la operación efectiva de una parte de la Organización
[pc] pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización

1 - 2	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[pd] persecución de delitos	
6 - 10	Impida la investigación de delitos graves o facilite su comisión
1 – 5	Dificulte la investigación o facilite la comisión de delitos
[trs] tiempo de recuperación del servicio	
9 –10	RTO < 4 horas
7 – 8	4 horas < RTO < 1 día
4 – 6	1 día < RTO < 5 días
1 – 3	5 días < RTO

Fuente: (Magerit, 2012)

ANEXO N° 5: Catálogo de amenazas por activo y dimensión de seguridad de la información

[N]	Desastres naturales			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[N.1]	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[N.2]	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[N.*]	Desastres naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. Se excluyen desastres específicos tales como incendios Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la Indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I]	**De origen industrial**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[I.1]	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I.2]	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I.*]	Desastres industriales	Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc. Se excluyen amenazas específicas como incendio por cuanto se ha previsto amenazas específicas.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones

		Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.		
[I.3]	Contaminación mecánica	Vibraciones, polvo, suciedad, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.4]	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.5]	Avería de origen físico o lógico	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. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	[D] disponibilidad	[SW] aplicaciones (software) [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.6]	Corte del suministro eléctrico	Cese de la alimentación de potencia	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información (electrónicos) [AUX] equipamiento auxiliar
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.8]	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente 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 al tráfico presente.	[D] disponibilidad	[COM] redes de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales	Interrupción de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante,	[D] disponibilidad	[AUX] equipamiento auxiliar
[I.10]	Degradación de los soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo	[D] disponibilidad	Media] soportes de información
[I.11]	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.	[C] confidencialidad	[HW] equipos informáticos (hardware) [Media] media [AUX] equipamiento auxiliar [L] instalaciones

		Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación		
[E]	**Errores y fallos no intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[E.1]	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	[I] integridad [C] confidencialidad [D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información
[E.2]	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	[D] disponibilidad [I] integridad [C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información
[E.3]	Errores de monitorización *(log)*	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	[I] integridad (trazabilidad)	[D.log] registros de actividad
[E.4]	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad	[D.conf] datos de configuración
[E.7]	Deficiencias en la organización	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. Acciones descoordinadas, errores por omisión, etc.	[D] disponibilidad	[P] personal
[E.8]	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	SW] aplicaciones (software)
[E.9]	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a	[C] confidencialidad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones

		donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.		
[E.10]	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	[I] integridad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[E.14]	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	[C] confidencialidad	
[E.15]	Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[E.18]	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[D] disponibilidad	D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[E.19]	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	[C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones [P] personal (revelación)
[E.20]	Vulnerabilidades de los programas (software)	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.	[I] integridad [D] disponibilidad [C] confidencialidad	[SW] aplicaciones (software)
[E.21]	Errores de mantenimiento / actualización de	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	[I] integridad [D] disponibilidad	[SW] aplicaciones (software)

	programas (software)			
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes electrónicos [AUX] equipamiento auxiliar
[E.24]	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	[D] disponibilidad	[S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[E.25]	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[E.28]	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	[D] disponibilidad	[P] personal interno
[A]	**Ataques intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[A.3]	Manipulación de los registros de actividad (log)		[I] integridad (trazabilidad)	[D.log] registros de actividad
[A.4]	Manipulación de la configuración	Afecta la configuración de los activos. Es diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad [C] confidencialidad [A] disponibilidad	[D.log] registros de actividad
[A.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, utilizando los privilegios de éste para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	[C] confidencialidad [A] autenticidad [I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.6]	Abuso de privilegios de acceso	Cada usuario utiliza 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, puede ocasionar problemas.	[C] confidencialidad [I] integridad [D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones

[A.8]	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	[SW] aplicaciones (software)
[A.9]	[Re-]encaminamiento de mensajes	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. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Un ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	[C] confidencialidad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.10]	Alteración de secuencia	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.	[I] integridad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	[C] confidencialidad [I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[A.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.	[C] confidencialidad	[COM] redes de comunicaciones
[A.13]	Repudio	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.	[I] integridad (trazabilidad)	S] servicios [D.log] registros de actividad

[A.14]	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	[C] confidencialidad	[COM] redes de comunicaciones
[A.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	[I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[A.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	[D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [Media] soportes de información [L] instalaciones
[A.19]	Revelación de información	Revelación de información (divulgación, copia ilegal de software)	[C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[A.22]	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	[C] confidencialidad [I] integridad [D] disponibilidad	[SW] aplicaciones (software)
[A.22]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	[C] confidencialidad [D] disponibilidad	[HW] equipos [Media] soportes de información [AUX] equipamiento auxiliar
[A.24]	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada (saturación del equipo informático)	[D] disponibilidad	[S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[A.25]	Robo	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 más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que	[D] disponibilidad [C] confidencialidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar

		establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.		
[A.26]	Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. (destrucción de hardware o de soportes)	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[A.27]	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	[D] disponibilidad [C] confidencialidad	[L] instalaciones
[A.28]	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. (daños a la disponibilidad del personal)	[D] disponibilidad	[P] personal interno
[A.29]	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	[C] confidencialidad [I] integridad [D] disponibilidad	[P] personal interno
[A.30]	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	[C] confidencialidad [I] integridad [D] disponibilidad	[P] personal interno

Fuente: Elaboración propia, adecuado de (Magerit, 2012)