UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS Y SISTEMAS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CICLO ACADÉMICO 2017 - 2019

Tesis para optar al título de

Master en Gestión de la Seguridad de la Información

"PROPUESTA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, EN LA DIRECCIÓN GENERAL DE INGRESOS, BASADO EN EL ESTÁNDAR ISO 27005"

Autor: Ing. Carlos Alberto Carrillo López # 2017-0002M

Tutor: Msc. Evelyn Espinoza Aragón

Managua, Nicaragua 2019

INDICE

Anexo 1

Causas	Riesgos	Consecuencia	Clasificación	Identificación del Riesgo
Medios o circunstancia	Evento que generara un impacto	Resultado que se pueden presentar	De acuerdo a su característica	Resultado esperado
Descripción a adecuada de los Riesgos				

Anexo 2

Criterio y caracteristica de activos										
ID Activo	Activo	Propietario	ubicación	Amenaza	Vulnerabilidad	Impacto			Probabilidad	Riesgo
						C	I	A		
DGI-001-2019	SERVIDOR PRODUCCION	JUAN PEREZ	CENTRO DE DATOS	VIRUS	ANTIVIRUS DEBIL	2	3	1	1	3
DGI-002-2019	SERVIDOR DE ARCHIVO	MIGUEL HERNANDEZ	CENTRO DE DATOS	VIRUS	ANTIVIRUS DEBIL	3	3	3	1	4
DGI-003-2019	CONTRATOS PROVEEDORES	JUAN PEREZ	ADQUISICION	DIVULGAR	ACCESO NO CONTROLADO	4	4	1	2	5
DGI-004-2019	PORTATIL	MILTON MARTINEZ	FINANZAS	ROBO	FALTA DE SEGURIDAD	5	4	3	2	6

77

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

“PROPUESTA DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION, EN LA DIRECCION GENERAL DE INGRESOS, BASADO EN EL ESTANDAR ISO 27005”

Agradecimientos

Gracias a Dios por permitir estar ante todos mis logros, a mi familia por ser parte de este proceso de formación.

A la Dirección General de Ingresos por el apoyo brindado en cada momento y hacerme partícipe de esta Maestría.

A cada una de las personas que fueron participes de este proceso, ya sea de manera directa e indirecta, brindaron su aporte para verse reflejado en esta culminación.

Presentación

El trabajo será desarrollado en base a una propuesta de gestión de riesgo de seguridad de la información, basado en el estándar ISO 27005, para la Dirección General de Ingresos (DGI).

Conociendo la necesidad de mejorar la gestión de riesgo de la información en la DGI, se realizará un estudio previo para que apoye particularmente los requisitos del sistema de gestión de seguridad de la información, aportando a la institución estrategias de avances que optimicen resultados.

Se tomarán en cuenta definiciones vinculadas a la disminución de vulnerabilidad en situaciones de riesgos, enfocado a las directrices que expresa la norma ISO 27005, así como políticas y procesos de gestión de riesgos, a través de los mecanismos de la norma ISO 27005 se determinaran los factores que incidirán en la aceptación de esta gestión de riesgos en la seguridad de la información, y se identificaran los activos de información críticos de la DGI, con el fin de definir su alcance.

A través de la investigación y del análisis efectuado en los procesos de información, se podrá observar la importancia de la gestión de riesgo para garantizar la confidencialidad, integridad y disponibilidad de la información, lo que obtendrá mayor eficacia en el monitoreo y cumplimiento de los planes de acción definidos.

CAPITULO I. GENERALIDADES

1. Introducción

Hoy en día, la seguridad en la información se ha convertido en el bastión de las operaciones para las instituciones, ayudando a definir el rumbo que tiene que seguir.

Las instituciones, dependen en su totalidad de poseer la información integra y estar disponible en el momento exacto de su requerimiento, garantizando la disponibilidad y confidencialidad de la misma.

Al pasar del tiempo la información ha tomado una gran importancia siendo así el principal activo para la toma de decisiones, y es aquí donde surge la necesidad de poder desarrollar continuamente, nuevas tecnologías con el principal objetivo de proteger la información contra cualquier riesgo que desencadene un impacto negativo en el plan estratégico de la institución.

Para la DGI resulta evidente la importancia de la información y la prioridad de planes de contingencias, que permitan manejar de la mejor manera posible las situaciones que impidan la continuidad del negocio. Para su éxito, es necesario que tengan debidamente identificados todos aquellos activos de información, para el desarrollo de sus funciones y actividades e incluya políticas y controles específicos para el manejo de este tipo de activo.

Existen riesgos que por su naturaleza no pueden evitarse, pero si pueden ser mitigados mediante medidas que garanticen la preservación y disponibilidad de la información de carácter esencial y que esta no se pierda de forma definitiva, así como

eventos que pueden causar desastres que producen la naturaleza y los seres humanos, ya sea de una forma accidental o malintencionada.

La aplicación de estrategias y diseños permitirán identificar todos los eventos potenciales, capaces de afectar y poder gestionar los riesgos, creados con el fin de tener una consonancia con el apetito al riesgo.

Para esto es importante ajustar un marco de trabajo en el estado actual de la institución aplicando conceptos y propósitos relacionados con la gestión de estos riesgos basándose en la ISO 27005, aplicando mecanismos de mejoras para poder fortalecer las decisiones en respuestas a los riesgos y poder reducir pérdidas de operaciones.

2. Planteamiento del Problema

Actualmente la DGI ha avanzado en cuanto a tener un sistema de seguridad de la información más eficaz, sin embargo, es necesario ajustar los que ya existen, que permita validar los posibles riesgos antes situaciones de vulnerabilidad y amenazas, lo que contribuiría al funcionamiento de sus operaciones y mayores controles en la seguridad de la información.

Los procesos actuales existentes, deben ajustarse con mayores controles, que garanticen la disponibilidad, confidencialidad e integridad de la información de manera continua, descartando así la identificación de reducir o eliminar las probabilidades del riesgo.

Mejorar una gestión de riesgo de seguridad de la información para la DGI, permitirá tener objetivos alineados a mecanismos, acciones y evaluaciones, para la identificación del riesgo antes que ocurran, administrando de esta manera la pérdida de operaciones.

3. Antecedentes

Para la realización de esta investigación se tomará como referencia, lo que establece la Norma Sobre Gestión de Riesgo Tecnológico, Resolución No. CD-SIBOIF-500-1 SEP19-2007, la Guía Especializada para las Normas Generales de Control Interno en Evaluación de Riesgos de la Contraloría General de la Republica de Nicaragua y como legislación comparada las Normas Técnicas de Costa Rica (INTECO) INTE/ISO/IEC 27005 relacionadas las directrices para Gestión del Riesgo de la Seguridad de la Información, apoyándose en los conceptos generales establecidos en INTE/ISO/IEC 27001, diseñada para apoyar la implementación satisfactoria de la seguridad de la información, basada en enfoque de gestión de riesgo.

En el cual se hace mención en la norma ISO 27005 que la gestión del riesgo de la seguridad de la información debería contribuir con lo siguiente:

- ✓ Identificar los riesgos
- ✓ Que los riesgos se valoren en términos de sus consecuencias para el negocio y la posibilidad de su ocurrencia
- ✓ La posibilidad de ocurrencia y las consecuencias de estos riesgos sean comunicadas y entendidas
- ✓ Establecer un orden de prioridad para el tratamiento del riesgo
- ✓ Priorizar las acciones para reducir la ocurrencia de riesgos
- ✓ Que las parte interesadas se involucren cuando se tomen decisiones de gestión del riesgo y a que se mantengan informadas sobre el estado de la gestión del riesgo
- ✓ La efectividad del seguimiento del tratamiento del riesgo

- ✓ Que se les dé seguimiento y sean revisado regularmente los riesgos y le proceso de gestión
- ✓ Recolectar información para mejorar el enfoque de la gestión del riesgo
- ✓ Que los gerentes y el personal sean educados acerca de los riesgos y las acciones tomadas para mitigarlos.

El proceso de gestión del riesgo de la seguridad de la información puede aplicar a la organización como un todo, a cualquier parte específica de la organización, a cualquier sistema de información existente o planificada, o aspectos particulares de control. (INTECO, 2012).

Así mismo para la investigación, será fundamental contar con información relevante plasmada por Y. Tibaquira Cortes (2015) en su tesis sobre Metodología de Gestión de Incidentes de Seguridad de la Información y Gestión de Riesgos para Plataforma SIEM de una Identidad Financiera Basada en la Norma ISO/IEC 27035 e ISO/IEC 27005.

4. Justificación

La DGI en el marco de su estrategia, ha implementado como política institucional, la modernización y ampliación de la tecnología a través de desarrollo en los sistemas informáticos que mejoren la gestión fiscal, y que facilite el cumplimiento voluntario de la obligación tributaria de los contribuyentes, así como la ejecución de medidas de seguridad informática, que permita una disminución de los riesgos asociados a la seguridad de la información.

Por tal razón el presente trabajo se enfocará en la gestión de riesgos de seguridad de la información acorde a los procesos actuales, con la finalidad que sean mejorados y avalados por el más alto nivel, para su ejecución según los intereses institucionales.

Esta gestión, implicara una metodología, a través de una serie de procesos que permita gestionar de manera más eficiente la información en los niveles de riesgos definidos, así como el alcance y los criterios de probabilidad a fin de seguir identificando las necesidades de la institución, en el cumplimiento de los requisitos de un sistema de gestión de seguridad de la información, para obtener mayor confidencialidad, integridad y disponibilidad de la información.

5. Objetivos

5.1 Objetivo General

Ajustar un marco de trabajo para la implementación de un procedimiento de gestión de riesgo de seguridad de la información, basados en el estándar ISO 27005 y políticas institucionales para las operaciones de la Dirección General de Ingresos.

5.2 Objetivos Específicos

- ✓ Analizar los factores externos e internos, que intervienen en la aceptación de una gestión de riesgo, en la Dirección General de Ingresos.
- ✓ Establecer un procedimiento para identificar los riesgos, amenazas y vulnerabilidades, para los activos de información.
- ✓ Definir los planes para mitigación, tratamiento y eliminación de riesgos residuales.

6. Diseño Metodológico

La investigación será de tipo documental y aplicada a una institución, a través de la recopilación, revisión y análisis de la información, que podrá ayudar a una correcta implementación de mejores prácticas de sistema de riesgos en la tecnología de la información.

El desarrollo de dicho trabajo, iniciara a partir del análisis sobre la situación actual en los modelos implementados en la seguridad de la información institucional, sus políticas, planes y procesos, así como los controles que estos poseen en cada uno de los niveles para mejorar su estado de vulnerabilidad y que tenga un impacto positivo en los objetivos institucionales.

Como técnicas se definirán mecanismo y directrices para la aplicación de este sistema tomando como base la norma ISO 27005, que conlleven a la toma de decisiones frente al riesgo ocasionado por el incidente, según los criterios definidos para la gestión de riesgos, que puedan generarse al momento de su implementación.

Se identificarán los principales activos de la información, a través de un análisis de riesgos de información seleccionada, para disminuir las ocurrencias de las probabilidades de riesgos, obteniendo una matriz.

Se realizará análisis de las prácticas internacionales de gestión de riesgo, con el objetivo de validar procesos más adecuados, que puedan ser aplicados, según el patrón del sistema de seguridad de la información que existe en la actualidad en la institución.

La investigación será de tipo no experimental, y según su enfoque estará basado en un análisis cualitativo de la información, ya que dicho estudio no usara variables, sino,

se analizarán los fenómenos en su ambiente de desarrollo, y por su grado de conocimiento será de tipo descriptivo.

7. Alcance o Metas

- Definir los mecanismos y directrices, bajo norma ISO 27005, acorde a los procesos existentes.
- Detallar el alcance del proceso de gestión de riesgo de seguridad de la información.
- Compilación de información acerca de la organización, para determinar el entorno en el que opera y su relevancia con respecto al proceso de gestión del riesgo de la seguridad de la información.

CAPITULO II- MARCO DE REFERENCIA

2.1. Marco Teórico

2.1.1. Gestión de riesgo.

Según Gerber y von Solms (2005), proponen adoptar un enfoque alternativo al análisis de riesgos tradicional, en el cual se analicen no solamente los riesgos de los activos tangibles, sino también los riesgos de los intangibles como la información; además, consideran relevantes los riesgos causados por asuntos culturales, legislativos, sociológicos, entre otros.

Asimismo, Lategan y von Solms (2006), enfatizan en que las empresas hoy en día, deben asegurar que los riesgos sean gestionados holísticamente y que la terminología y prácticas de riesgo relacionados con TICs estén congruentemente alineadas con la terminología y prácticas de las empresas. Es decir, las TICs no pueden ser vistas como un componente independiente en cuanto a la gestión de riesgos se refiere.

2.1.2 Importancia de una gestión de riesgos.

José Silva (2017), nos dice que: “Las organizaciones están expuestas a numerosos riesgos. La gestión de estos, comienza detectando los posibles peligros a los que se exponen, para después adoptar las medidas oportunas e implantar los procesos necesarios para minimizar o eliminar esos peligros.

Hay que darle a esta gestión la importancia que se merece, porque puede afectar las operaciones diarias de la organización traduciéndose en pérdidas. Por eso además de la responsabilidad y convicción de directores y altos ejecutivos, los reguladores están

exigiendo, a las empresas bajo su supervisión, adoptar políticas y estructuras para el control de los riesgos a los que se enfrentan."

2.1.3 Tecnología de información.

Jorge Lañez (2010), afirmo que "las TI están enormemente vinculadas a los resultados de negocio de las empresas y eso contribuye a generar mayor entendimiento y confianza entre los ámbitos de negocio y de TI" y desgranó, entre los beneficios del Gobierno TI logrados por su propia empresa, "mayor contribución a la innovación del negocio, mayor flexibilidad de la organización TI, un aumento de la fiabilidad y rendimiento de los servicios, y una mejora en la ejecución de los proyectos.

Por su parte, Francisco Souto (2010), aseguro aseguró que "el Gobierno TI es esencial" y resaltó que, de forma combinada a la Gestión TI, "comporta una visión más ágil y unas líneas de trabajo muy definidas para poder solventar problemas clásicos de las TI como su integración con el negocio, la consecución de niveles de servicio o el cumplimiento regulatorio".

2.1.4 Seguridad de la información.

Según ISO 27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:

- ✓ Electrónicos
- ✓ En papel
- ✓ Audio y vídeo, etc.

La seguridad de la información consiste en asegurar que los recursos del sistema de información de una empresa, se utilicen de la forma que ha sido decidido y el acceso a su contenido, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

2.1.5 ISO 27005.

La primera versión de la norma fue publicada el 4 de junio del 2008, en ella se definen los lineamientos para la gestión del riesgo en la seguridad de la información, sin separarse de los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

La ISO 27005 es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la seguridad de la información de la organización.

No obstante, como otras normas ISO y sistemas basados en procesos, un método considerado válido y por lo tanto recomendable, es establecer un proceso de gestión que se enfoque en la mejora continua PHVA (Planificar, Hacer, Verificar y Actuar).

2.1.6 Modelo PHVA.

Yuli Sánchez (2017), se refiere a que el modelo PHVA constituye una de las principales herramientas de mejoramiento continuo en las organizaciones, utilizada

ampliamente por los sistemas de gestión de la calidad (SGC) con el propósito de permitirle a las empresas una mejora integral. Siguiendo el siguiente esquema:

Planificar: Se establecen los planes estratégicos, abordando los objetivos, procesos y procedimientos para la gestión del riesgo tecnológico, con el fin de conseguir unos resultados acordes con las políticas globales de la organización.

Hacer: Corresponde a la implementación y operación de los controles, procesos y procedimientos e incluye la operación e implementación de las políticas definidas.

Verificar: Se trata de evaluar y medir el desempeño en la estructura de riesgo implementando medidas de seguridad e informar sobre los resultados.

Actuar: Consiste en establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos.

2.1.7 Evaluación del riesgo.

Según INTE/ISO/IEC 27005, la evaluación del riesgo cuantifica o describe cualitativamente el riesgo y permite a los gerentes priorizarlos de acuerdo con la gravedad percibida o con otros criterios establecidos, tomando en cuenta cada uno de los pasos de la evaluación.

2.1.7.1 La valoración del riesgo.

Determina el valor de los activos de información, identifica las amenazas correspondientes y las vulnerabilidades que existen (o podrían existir), identifica los controles existentes y sus efectos en el riesgo identificado, determinar las consecuencias potenciales y existentes y sus efectos en el riesgo identificado, determina las

consecuencias potenciales y prioriza los riesgos derivados y los ordena según el conjunto de criterios evaluados.

2.1.7.2 Identificación del riesgo.

El propósito de la identificación del riesgo es determinar que podría suceder para causar una pérdida potencial, y para conocer mejor cómo, cuándo y por qué la pérdida podría suceder. La identificación debería de incluir riesgos, ya sea que su origen este o no, bajo el control de la organización, aun cuando el origen o causa puedan no ser evidentes.

2.1.7.3 Análisis del riesgo.

El análisis del riesgo se puede llevar a cabo en diferentes grados de detalle dependiendo de la criticidad de los activos, el alcance de las vulnerabilidades conocidas, y los incidentes anteriores relacionados con la organización.

2.1.8 Evaluación de riesgos.

Para la realización de una evaluación efectiva de riesgos en la seguridad de la información se considera tanto en los temas organizacionales como en los técnicos, por lo que es necesario examinar como las personas emplean la infraestructura de forma diaria. La evaluación es de vital importancia para cualquier iniciativa de mejora en seguridad, por este se genera una visión a lo ancho de la empresa de los riesgos de seguridad de la información, se provee de una base para mejorar.

Para que las organizaciones comprendan que eventos potenciales impactan en los logros de los objetivos establecidos institucionalmente.

2.1.9 Identificación de activos.

La norma ISO 27005, nos menciona que la identificación de activos se debería de realizar a un nivel adecuado de detalle que provea información suficiente para la valoración del riesgo. El nivel de detalle utilizado en la identificación del activo va a influir en la cantidad total de información recolectada durante la valoración del riesgo. El nivel se puede refinar en interacciones adicionales de la valoración del riesgo.

Se debería de identificar el dueño de cada activo, a fin de proporcionar responsabilidad y rendición de cuentas para el activo. El dueño del activo puede no tener derecho de propiedad sobre el activo, pero puede tener responsabilidad por su producción, desarrollo, mantenimiento, uso y seguridad según corresponda.

2.1.10 Tratamiento del riesgo.

La ISO 27005, nos menciona cuatro opciones disponibles para el tratamiento del riesgo:

2.1.10.1 Modificación del riesgo.

Se deberían de seleccionar controles apropiados y justificados para cumplir los requisitos identificados mediante la valoración del riesgo y el tratamiento del riesgo. Esta selección debería tomar en cuenta los criterios de aceptación del riesgo, así como también los requisitos legales, reglamentarios o contractuales.

2.1.10.2 Retención del riesgo.

Si el nivel del riesgo cumple los criterios de aceptación, no hay necesidad de implementar controles adicionales y el riesgo se puede retener.

2.1.10.3 Evitar el riesgo.

Cuando los riesgos identificados se consideran demasiado alto, o los costos de implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar completamente el riesgo, retirándose de una actividad o un conjunto de actividades planificadas o existentes, o cambiando las condiciones sobre las cuales opera la actividad.

2.1.10.4 Compartir el riesgo.

Compartir el riesgo conlleva una decisión de compartirlos con partes externas, puede crea nuevos riesgos o modificar los riesgos identificados existentes. Por lo tanto, puede ser necesario un tratamiento adicional.

2.2. Marco Conceptual

2.2.1 Riesgos.

Es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separados, no representan un peligro, pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.

2.2.2 Gestión de riesgo.

La gestión de riesgo es el proceso de identificar, analizar y responder a factores de riesgo a lo largo de la vida de un proyecto y en beneficio de sus objetivos. La gestión de riesgo adecuada, implica el control de posibles eventos futuros. Además, es proactiva, en lugar de reactiva.

2.2.3 Sistema de gestión de riesgo.

Los sistemas de gestión de riesgo están diseñados para identificar el riesgo. El sistema también debe poder cuantificar el riesgo y predecir su impacto en el proyecto. En consecuencia, el resultado es un riesgo aceptable o inaceptable. La aceptación o no aceptación de un riesgo depende, del nivel de tolerancia del gerente de proyectos por el riesgo.

2.2.4 Mitigación.

Reducción del valor monetario estimado de un riesgo al reducir la probabilidad de ocurrencia.

2.2.5 Aceptación.

Aceptar las consecuencias del riesgo. Con frecuencia, esto se cumple al desarrollar un plan de contingencia para ejecutar si el riesgo llega a ocurrir.

2.2.6 Prevención.

Eliminación de una amenaza específica, a menudo al eliminar la causa.

2.2.7 Activo.

Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo.

2.2.7.1 Activos tangibles.

Aquellos activos que contienen información, sobre los cuales se pueden tomar medidas preventivas y protegerlos sobre los riesgos físicos.

2.2.7.2 Activos intangibles.

Soportan la información dentro de un activo material, pueden inutilizar, aunque el activo no hay sufrido daño.

2.2.8 Amenazas.

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencia negativa sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

2.2.9 Vulnerabilidad.

Debilidad que presentan los activos y que facilita la materialización de las amenazas.

2.2.10 Impacto o consecuencia.

De la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradación que afecta el valor del activo, donde el cien por ciento seria la pérdida total del activo.

2.2.11 Probabilidad.

Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos).

2.2.12 Análisis del riesgo.

Consiste en averiguar el nivel de riesgo que la empresa está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

2.2.12 ISO 27005.

Estándar internacional que se ocupa de la gestión de riesgos de seguridad de información.

2.2.13 Confidencialidad.

La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.

2.2.14 Integridad.

La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.

2.2.15 Disponibilidad.

La información debe estar siempre accesible para aquellos que estén autorizados.

CAPITULO III- FACTORES EXTERNOS E INTERNOS EN LA GESTION DE RIESGO

3.1 Principales procesos y actividades

Es esencial que los administradores de riesgo dentro de la institución, conozcan los servicios de la organización, de hecho, el tipo de servicios producidos por la institución tendrán un gran impacto en su modelo de negocio y como la institución lleva a cabo sus negocios. Además, los productos y servicios pueden permitir que la institución pueda estar expuesta a riesgos especiales, ejemplos de estos ambientales y enjuiciamiento o legales.

Es importante que los administradores comprendan los procesos de negocio de la institución, ya que esta conducta, es la que expone a la organización a numerosos riesgos para la seguridad de la información. El administrador del riesgo debería analizar y comprender la naturaleza de estos procesos y determinar los riesgos directos e indirectos a los que la organización está expuesta, durante las operaciones tal como se hizo en el análisis de riesgo.

3.2 Factores externos

Las instituciones del sector público en Nicaragua para poder cumplir sus objetivos institucionales, se enfrentan a diferentes tipos de riesgos en entornos ya sean sociales, políticos, legales y reglamentarios. Que de alguna manera se encuentran relacionados con la administración de recursos públicos.

La DGI, se rige en gran manera por los fines y objetivos institucionales de conformidad con ordenamientos jurídicos y controles internos institucionales, regulado por la Contraloría General de la Republica.

La Contraloría General de la Republica, provee herramientas o mecanismos para el establecimiento e implementación de la gestión de riesgo, con el principal objetivo que las instituciones no puedan ser afectadas en el cumplimiento de sus objetivos y los del estado en beneficio de la comunidad.

Así mismo la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF) establecen normas de suma importancia que las instituciones deben cumplir en la gestión de riesgo, donde permita poder identificar, medir, limitar, controlar y catalogar cada uno de los riesgos a lo que las instituciones se enfrentan. Los cuales pueden ser generados por fallas en los procesos internos, en la tecnología de la información, en el recurso humano (personas) o por ocurrencia de eventos externos.

Para las instituciones públicas como la DGI, existen factores que intervienen grandemente en una gestión de riesgo, como:

3.2.1 Económico

Es uno de los elementos más importante al momento de una implementación de una gestión de riesgo, debido a que cuenta con un determinado presupuesto aprobado, el cual interviene en los planes de contingencia que puedan ejecutarse al momento de poder dar una respuesta inmediata a la mitigación de un riesgo si este no ha sido incorporado dentro del presupuesto aprobado. Así mismo las decisiones de políticas económicas, de las deudas públicas, como los cambios de las políticas fiscales para el

cumplimiento de los objetivos principales de la institución, podrían verse afectado grandemente.

3.2.2 Ambiental

Pueden surgir condiciones que escapan del control directo de la finalidad de la implementación de la gestión de riesgos, las circunstancias que rodean su ejecución como: cultura, estructura y gobierno de la institución, al mismo tiempo puede existir la disponibilidad y distribución de instalaciones, recursos, infraestructura. Así como las normas, políticas, métodos y procedimientos internos.

3.2.3 Tecnológico

Es uno de los factores que juega un rol importante en la gestión de riesgo, debido a que influye en gran manera en los niveles de desarrollo tecnológico, como los grados de implantación de tecnologías de la información, o de obsolescencia tecnológica, este factor depende grandemente del factor económico o del presupuesto que tiene aprobado la institución para el cumplimiento de sus objetivos y alcance.

3.2.4 Políticos y legales

En vista que es una institución de gobierno, no anuente a los tipos y características del sistema político vigente, así como el nivel de estabilidad, las políticas monetarias y financiera, que pueden ser tomadas en cuenta en una evaluación actual y futura.

Dentro del contexto legal, podría afectar las adecuaciones a leyes y normativas (tributarias, laborales, etc.), que pudieran afectar a la institución y la operatividad de la misma.

3.2.5 Social

Se puede ver afectada por el comportamiento de usuarios, la responsabilidad social, cambios culturales. Así como los valores sociales, morales, éticos.

3.3 Factores internos

En la DGI existen diferentes tipos de factores internos que son de gran importancia al momento que se realice la implementación de una gestión de riesgo y que conforman el cumplimiento principal de toda institución como son:

3.3.1 Infraestructura

Las instituciones de gobierno, deben de procurar disminuir al máximo los gastos, asignando los recursos de manera eficiente, además cumplir con el plan estratégico institucional.

Su principal objetivo es proporcionar una imagen completamente transparente respecto a los activos de infraestructura, ubicación, valor, cantidad entre otros.

La propuesta de una gestión de riesgo en lo que se refiere a infraestructura en la DGI, ayudara a realizar un correcto análisis y asignación de todos aquellos elementos críticos. Al mismo tiempo poder tener debidamente identificados cada uno de los activos, así como su capacidad y la disponibilidad de los mismos; garantizando en gran manera la entrega de servicios y atención adecuada a todos aquellos usuarios que lo requieran.

3.3.2 Personal

Es necesario considerar el talento humano dentro de la institución, debido a que es un factor importante, se tiene que valorar los perfiles de desempeño de cada uno de los usuarios, obteniendo personal cualificado y profesionales que ejerzan las funciones

encomendadas, de esta manera se podría evitar, aquellos riesgos no intencionales o negligencia, así como ejercer las funciones correctamente por la falta de capacidad, y sobre todo cuando la conducta no cumple intencionalmente las normas o política de la institución.

3.3.3 Procesos

Se realizará una revisión de todos aquellos procesos existente dentro de la DGI, que ya se encuentran siendo utilizados, los cuales deberán demostrar el alcance de la institución, así como el cumplimiento de las actividades y funciones a favor de los objetivos estratégicos y su misión.

3.3.4 Tecnología

Todo lo relacionado a la tecnología se tendrá un trato muy importante en vista que de estos son los activos más importantes dentro de la institución, donde es necesario poder garantizar la continuidad de negocio, además la confidencialidad, integridad y disponibilidad de la información.

Los sistemas informáticos inadecuados o mal estructurado, puede ser perjudicial para la DGI, hasta el punto de poder generar incidentes como:

- ✓ Mal funcionamiento en las redes
- ✓ Caída de servidores
- ✓ Daño físico en los almacenamientos de datos
- ✓ Sistemas obsoletos
- ✓ Corte de energía por causas internas o externas
- ✓ Procesos de información lentos

CAPITULO IV - GESTION DE RIESGO PARA LOS ACTIVOS DE INFORMACION

4.1 Gestión de riesgo

Para la DGI los activos son de suma importancia debido a que estos son los que permiten desarrollar sus actividades y operaciones. La valoración sistemática ayuda a identificar necesidades de la institución en lo que se refiere a la seguridad de la información con el fin de poseer una gestión eficaz.

Poder gestionar los riesgos, permitirá controlar las amenazas o vulnerabilidad al que están expuesto los activos, así como prevenir la ocurrencia de daños a la institución y poder cumplir con los objetivos propuestos.

Para esto es necesario el correcto análisis de riesgos a través de una auditoria con el fin de poder identificar las vulnerabilidades actuales, con el fin de poder conocer las amenazas externas que impacte en las vulnerabilidades internas de nuestros procesos. No es solamente poder identificar como estamos que cantidad de incidencias y problemas existen, sino establecer los riesgos a los que están expuesto.

El análisis deberá de ser aplicado a los sistemas como a los procesos que ya se encuentran definidos, el objetivo principal es poder tener un resultado de todo el organigrama de operaciones con que cuenta la institución, para la comprobación del funcionamiento y los puntos que se requiere mejorar.

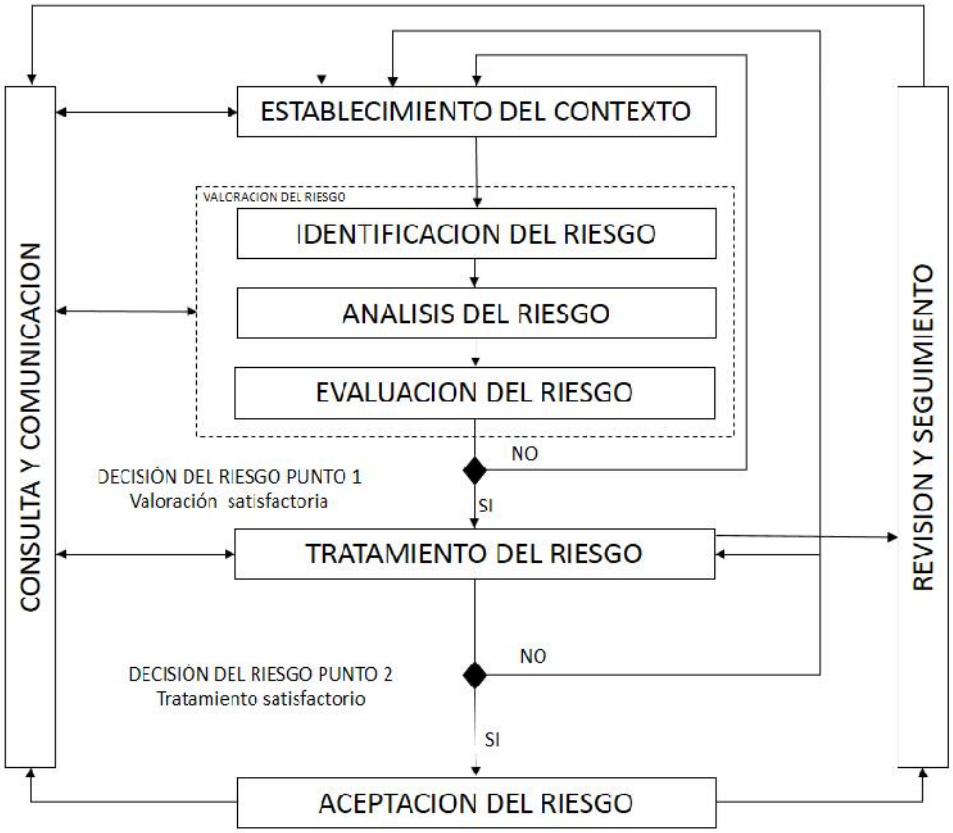
4.1.2 Establecer el contexto.

Para el cumplimiento de esta gestión de riesgos es necesario tener todo debidamente estructurado, con el objetivo de poder identificar, evaluar, medir y reportar las amenazas y oportunidades que afectan el alcance de los objetivos de la institución.

Cada uno de los servidores públicos de la institución son participe del aseguramiento del éxito del cumplimiento, pero es responsabilidad principal de las instancias superiores de la identificación y manejo.

Un control o manejo adecuado de los riesgos permite el perfeccionamiento de la institución, es importante establecer contexto en el que opera para poder tener una identificación, análisis, valoración y definición de las diferentes alternativas sobre el tratamiento del riesgo. Tomando en consideración las estrategias, valores institucionales, talento humano, estructura interna, políticas y objetivos con que cuenta la institución.

Ilustración 1 Proceso de gestión del riesgo de la seguridad de la información (ISO 27005:2011)



4.1.3 Identificación de riesgos.

La identificación de los riesgos debe efectuarse utilizando un proceso paso a paso, para incluir los riesgos de la institución, con este se logrará obtener una lista de todos aquellos eventos que podrían afectar a la institución, teniendo un mayor detalle para facilitar la caracterización de lo que puede suceder.

Es necesario utilizar técnicas como:

- ✓ Lista de chequeo
- ✓ Análisis de causa y efecto
- ✓ Diagrama de flujo
- ✓ Lluvias de ideas

El objetivo de la identificación del riesgo es conocer los sucesos que pueden producir en la organización y las consecuencias que puedan tener sobre los objetivos de la institución. Deben incluir riesgos, que no se originen bajo el control de la institución, puede implicar datos históricos, análisis, opiniones ya sean objetivas o expertas, así como aquellas necesidades de las partes interesadas, aun cuando el origen o causa puedan no ser evidentes. Anexo 1.

En este proceso se requiere de toda la participación del personal de las diferentes áreas y niveles.

4.1.3.1 Identificación de los activos.

Es necesario realizar los alineamientos básicos que deberán ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión de activos que son manejados por la institución. Tomando de esta manera las expectativas de las partes interesadas.

La identificación se debe de realizar a un nivel adecuado que proporcione información suficiente, además tenerlos debidamente separados para un mejor detalle e identificación de los mismos.

Se distinguen dos tipos de activos:

Tabla 1 Tipos de activos (PECB, 2015)

1. Activos Primarios	• Procesos del negocio y actividades • Informacion
2. Activos de soporte (dependen de los elementos primarios del alcance)	• Hardware • Software • Redes • Personal • Instalaciones • Estructura de la organización

Es recomendable tener los activos debidamente identificados con sus respectivos responsables, con el objetivo de proporcionar compromisos y rendición de cuentas para el activo.

El proceso de creación de un inventario de los activos es un requisito importante en la gestión de riesgo. El inventario de activos es esencial para establecer una protección eficaz y adecuada de los activos de la organización.

El inventario de activos deberá incluir toda la información necesaria para hacer la apreciación del riesgo, y en particular el tipo de propiedad, su propietario, su ubicación, información relativa a su protección. Anexo 2.

Si el inventario de los activos consiste en varios registros, debería evitarse la duplicación innecesaria de información para asegurar una alineación del contenido.

El inventario puede ser de gran ayuda con otros fines dentro de la institución como la contratación de un seguro o motivos financieros contables.

Pueden existir caso que los dueños no tienen derecho de propiedad sobre el activo, pero pueden tener responsabilidades por las funciones (producción, desarrollo, mantenimiento, uso y seguridad) según asignación de funciones. Ver Tabla 2.

Tabla 2 Identificación de los Activos de Soporte (PECB, 2015)

CATEGORIA	DEFINICION	EJEMPLOS
Hardware	Todos los elementos físicos de soporte a los procesos	Servidores, ordenadores, portátiles
Software	Todos los programas que contribuyen al tratamiento de datos	Sistemas operativos, programas, aplicaciones para usuarios
Redes	Todos los dispositivos de telecomunicaciones que interconectan físicamente remotos de un sistema de información	Router, switch, firewall
Personal	Todo el personal involucrado en las operaciones y/o procesos	Propietarios, programadores
Sitios	Lugares físicos donde se llevan a cabo las operaciones	Edificios, centros de datos, mobiliario y equipo de oficina
Estructura de la organización	Marco organizativo asignado para la realización de las actividades	Direcciones, oficinas y departamentos

La identificación de los activos de información, permite clasificarlos y poder brindar una mayor protección, identificando sus características y rol en un determinado proceso.

Es necesario la conformación de un equipo, que determine los activos que serán parte del inventario, además deberán estar involucrados todos los líderes de cada proceso, estos últimos deberán solicitar la revisión de la definición de los activos por parte del usuario del activo que tienen asignado, para que sea validada si son las partes interesadas.

4.1.3.2 Determinación de los valores de los activos.

La institución deberá de definir sus propios parámetros para la escala de valores de los activos, decidiendo enteramente sobre el valor de un activo, es esencial que la

evaluación del valor de los activos se formule en términos adecuados para que los contactos obtengan información relevante. Ver Tabla 3.

Tabla 3 Escalas de los valores de los activos

ESCALA	VALOR DE LOS ACTIVOS
INSIGNIFICANTES	**0**
BAJO	**1**
MEDIO	**2**
ALTO	**3**
MUY ALTO	**4**

La escala de valores debe integrar las diferentes propiedades que puedan afectar a la confidencialidad, integridad y disponibilidad de los activos importantes, además considerar las dependencias con otros activos.

Los términos típicos utilizados para la valoración cualitativa de los activos incluyen palabras tales como: insignificantes, muy bajo, bajo, medio, alto, muy alto. La elección y los rangos de términos adecuados para la institución dependen de las necesidades de seguridad de la institución.

4.1.3.2.1 Criterios de valoración.

Los criterios utilizados como base para asignar un valor a cada activo se deberán de escribir en términos no ambiguos. Esto debido a que algunos de estos valores tienen que ser determinados subjetivamente y probablemente intervienen muchas personas en su determinación.

Otra base de valoración de los activos, es el costo debido a la perdida de confidencialidad, integridad y disponibilidad como consecuencia de un incidente. Se deberá de considerar también, el no repudio, la rendición de cuentas, la autenticidad y

la confiabilidad, según corresponda. Anexo 3. Esta valoración sería un elemento importante para dimensionar el valor del activo, además del costo de reposición, basado en estimaciones de las consecuencias adversas para los objetivos de la institución.

Muchos activos pueden tener varios valores asignados durante el curso de la valoración. el valor asignado puede ser el máximo de todos los valores posibles o puede ser la suma de todos o de algunos de los valores posibles.

4.1.3.2.2 Reducción a una base común.

Todas las valoraciones de activos necesitan ser reducidas a una base común. Esto se puede llevar a cabo con la ayuda de criterios como:

- Violación de la legislación y/o regulación
- Deterioro del desempeño de la institución
- Pérdida de credibilidad/efecto negativo sobre la imagen
- Incumplimiento relacionado con información personal
- Peligro de la seguridad personal
- Efectos adversos sobre la aplicación de la ley
- Incumplimiento de la confidencialidad
- Incumplimiento del orden publico
- Perdida financiera
- Interrupción de las actividades comerciales
- Peligro de la seguridad ambiental

4.1.3.2.3 Escala de valoración.

La institución deberá de llegar a un acuerdo sobre la escala a utilizar en toda la institución. El primer paso es decir ir el número de niveles que se deben utilizar. No existe reglas con respecto al número de niveles más adecuado. Cabe mencionar que demasiado nivel hace difícil las decisiones coherentes.

Estos límites pueden ser evaluados de acuerdo a los criterios seleccionados, dependiendo de la consecuencia que podría ser desastrosa o incluso insignificante para la institución.

4.1.3.2 Identificación de amenazas.

Las amenazas pueden ser de origen natural o humano, y accidentales o deliberadas, las cuales pueden afectar los activos de información, procesos y sistemas de la institución. Estás pueden surgir desde la parte externa o interna de la institución, pueden afectar a más de un activo, causando impacto diferente dependiendo de qué activo fue el afectado. Anexo 4.

La identificación y estimación de la posibilidad de ocurrencia de las amenazas puede ser obtenida por los usuarios o responsables de los activos, así como el personal que es de conocimientos de cada uno de los procesos o entorno que tienen asignados.

4.1.3.3 Identificación de los controles existente.

Es importante para el proceso de gestión de riesgo la identificación de los controles existentes y los planificados que existen dentro de la institución, con el principal objetivo de no realizar un duplicado de los mismos. Realizar la verificación en cada uno de los controles si estos están siendo trabajados correctamente, esto con el objetivo que si un control no está realmente siendo ejecutado puede causar una vulnerabilidad en el

proceso, es necesario que al momento de su verificación un control no está siendo operado o este falle, que exista un control complementario para tratar el riesgo identificado.

Todos aquellos controles que están planificados para su incorporación deberán ser agregados según el plan de tratamiento de riesgo de acuerdo a los que ya están implementados.

Algunos de los controles están relacionados a:

- Políticas de seguridad
- Responsabilidades
- Procedimientos
- Control de incidentes
- Continuidad de operaciones
- Protección y manejo de información

Se presentan una característica que hay que tomar en cuenta para la definición de los controles:

Característica	Descripción
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad

Periódicos	Tienen frecuencia de aplicación en el tiempo
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo
Asignables	tienen responsables definidos para su ejecución

Es recomendable realizar algunas actividades al momento de su identificación como la revisión de los documentos que contengan información acerca de los controles, las personas responsables de las diferentes dependencias involucradas en la seguridad de la información y de los sistemas, realización de una validación o comparación de aquellos controles que se ha estado ejecutando correcta y efectivamente, a esto se puede incluir los resultados de las auditorias que se han realizado.

Para un mejor detalle de los controles de seguridad existentes y previstos, se puede utilizar la lista de controles de seguridad de la norma ISO 27001. Anexo 5.

4.1.3.4 Identificación de vulnerabilidades.

Para mejorar la realización de la identificación de vulnerabilidades en cualquier negocio, es necesario contar con las amenazas ya conocidas, así como listas de activos y controles existentes, tomando en cuenta que la vulnerabilidad es debilidad que pueden tener los activos de información y controles que son explotados por una amenaza. Ver Tabla 4.

Tabla 4 Tipos de Vulnerabilidades (PECB, 2015)

CATEGORIA	EJEMPLOS
Hardware	Falta de mantenimiento
	Portabilidad
Software	No hay registro de auditoria
	Interfaces complejas
Red	Falta de cifrado de las transferencias
	Único Punto de Acceso
Personal	Falta de capacitación
	Falta de supervisión
Sitio	Sitio en una zona susceptibles de inundaciones
Estructura organizativa	Falta de segregación de tareas
	No hay una descripción de las funciones

Remarcar que un control incorrectamente implementado, funcionando mal o utilizado incorrectamente puede ser una vulnerabilidad.

Las vulnerabilidades a nivel general pueden ser identificadas en las siguientes áreas:

- ✓ Organización
- ✓ Procesos y procedimientos
- ✓ Rutinas de gestión
- ✓ Personal
- ✓ Entorno físico
- ✓ Configuración de sistemas de información
- ✓ Hardware, software o equipos de comunicaciones
- ✓ Dependencias de partes externas

El objetivo es poder determinar la vulnerabilidad específica en los activos incluidos en cada proceso. Las vulnerabilidades se analizan generalmente con las mismas personas responsables que participaron en el estudio de los orígenes de las amenazas.

Muchas vulnerabilidades son asociadas a características negativas o positivas, que pueden tener efectos adversos.

4.1.3.5 Identificación de consecuencias.

Se debe de tener una lista de todos aquellos procesos ejecutados, un detalle de todos los activos, con su respectiva amenaza, con el objetivo de poder identificar las consecuencias en las cuales se ven involucrada la confidencialidad, integridad y disponibilidad. En el Anexo 6 se puede visualizar una lista de posibles consecuencias.

Hay que tomar en cuenta que una consecuencia puede generar inconformidad en las operaciones e inestabilidad en cada uno de los procesos, hasta la reputación y credibilidad.

Los daños o consecuencias que podrían darse por un escenario de incidentes, puede que exploten una cierta vulnerabilidad o conjunto de vulnerabilidades. Los incidentes pueden evaluarse de manera distintas en función de los que intervienen en la apreciación del riesgo. Los impactos significativos deben ser documentados.

Luego de la identificación de los activos bajo revisión, se debe tomar en cuenta los valores asignados mientras son evaluadas las consecuencias. Las valoraciones de los activos comienzan con la clasificación de activos de acuerdo a su criticidad en términos de la importancia, para cumplir con los objetivos del negocio de la institución.

Según la valoración de los activos se determina utilizando dos medidas:

- El valor de reposición del activo: el costo de recuperación y la sustitución de la información

- Las consecuencias en el negocio de la pérdida o compromiso del activo, así como las consecuencias potenciales adversas al negocio y/o legales o reglamentarias a causa de la divulgación, modificación, no disponibilidad y/o destrucción de información y de otros activos de información. (INTECO, 2012)

A continuación, se muestra una lista de varias posibles consecuencias que, o bien pueden afectar la disponibilidad, integridad, confidencialidad o una mezcla de las tres a la vez:

1. Perdida financiera
2. Pérdida de un activo o su valor
3. Procesamientos y sanciones
4. La pérdida de avance en la tecnología o en una técnica
5. La pérdida de eficacia o eficiencia
6. Violación de privacidad de los usuarios
7. Interrupción de servicio
8. Incapacidad para proporcionar el servicio
9. Perdida de reputación y credibilidad
10. Interrupción de las operaciones
11. Interrupción de las operaciones de grupos de interés externos
12. Las violaciones de leyes o reglamentos, o la incapacidad para cumplir obligaciones legales, juicios, contractuales, sanciones
13. Violaciones de políticas y procedimientos por parte del personal de seguridad y usuarios

4.1.4 Análisis del riesgo.

En el análisis del riesgo es necesario comprender la manera más detallada de abordarlo, debido a que se tomaran decisiones de cómo tratarlo y que métodos utilizaremos para el mismo. Conocer todos los factores que puedan influir en las causas y en las consecuencias. Tomando en cuenta que una situación puede tener muchas causas y consecuencias.

Considerar los controles de riesgos que deberíamos mejorar en la institución y la eficiencia de estos. Clasificándolos con el fin de establecer el nivel de riesgo y las acciones que se requieren implantar, para prevenir aún más el riesgo.

Debemos comprender las posibles consecuencias que puedan traer determinadas situaciones y la probabilidad que estas se produzcan con el objetivo de medir el nivel del riesgo. Tomando en cuenta los niveles de probabilidad y los posibles parámetros capaces de poder mejorar otras decisiones debidamente establecidas.

Para la institución es recomendable documentar y especificar cada una de las etapas para el proceso de Gestión de Riesgos, de ahí tendrán su propia guía con el objetivo de poder extender el alcance o revisión de los controles.

Los análisis deberán ser afines con los criterios de valoración del riesgo desarrollado, siendo esto parte del establecimiento del contexto. Los análisis pueden ser cualitativo o cuantitativo. Teniendo en cuenta la frecuencia con la que ocurren las amenazas la facilidad con la que puede ser explotada la vulnerabilidad.

De este modo las instituciones, mejoran de manera efectiva, centrándose de esta manera en los riesgos de alta prioridad.

El análisis cualitativo utiliza una escala de atributos calificativos en el cual se describe la magnitud de consecuencias potenciales (Baja, Media, Alta) y la probabilidad de que esas consecuencias puedan ocurrir.

Las definiciones de niveles de probabilidad e impacto pueden reducir la influencia de parcialidades, por lo que realizar el análisis cualitativo de riesgos es por lo general un medio rápido y económico de establecer prioridades para la planificación de las respuestas a los riesgos. También se sienta las bases para realizar el análisis cuantitativo, si se requiere.

El análisis cuantitativo es realizado primeramente sobre los riesgos definidos como prioritarios en el proceso, en el cual se analiza el efecto de esos riesgos, y les asigna una cuantificación numérica, lo que permite tomar decisiones en caso de incertidumbre.

4.1.4.1 Evaluación de consecuencias.

La norma ISO no establece como realizar un análisis de riesgo, pero es de suma importancia para toda institución evaluar las consecuencias y las probabilidades e identificar activos, amenazas y vulnerabilidades, esto con el objetivo de poder evaluar las consecuencias o el impacto que sufrirá la institución si el riesgo llegara a materializarse.

Para este aspecto se contará con una lista de escenarios de todos aquellos incidentes que están catalogados como relevantes, donde deberán estar identificadas las amenazas, vulnerabilidades, activos afectados, consecuencias a los activos y los procesos del negocio.

Cabe mencionar que la valoración de los activos es un factor importante en la evaluación del impacto en algunos escenarios de incidentes, debido a que puede afectar a más de un activo o solamente una parte de un activo.

El impacto inmediato puede ser tanto directo como indirecto

En el caso directo:

- ✓ Valor financiero de reposición por la pérdida del activo
- ✓ Costo de adquisición, configuración e instalación de nuevo activo o respaldo
- ✓ Costo de las operaciones suspendida debido al incidente hasta que el servicio proporcionado por el activo se restaure
- ✓ El impacto resulta en una violación de la seguridad de la información

En el caso indirecto:

- ✓ Costo de oportunidad
- ✓ Costo de interrupción de operaciones
- ✓ Potencial uso indebido de la información obtenida a través de una brecha de seguridad
- ✓ Violación de las obligaciones legales o regulatorias
- ✓ Violación de los códigos de conducta ética.

4.1.4.2 Evaluación de la posibilidad de incidentes.

Concluida la identificación de los posibles escenarios de incidentes y evaluación de sus defectos, es necesario determinar la probabilidad de cada uno de los escenarios y

los efectos que ocurren, utilizando análisis cualitativo o cuantitativo, tomando en cuenta la frecuencia con la que ocurren las amenazas y la facilidad con la que puede ser explotada la vulnerabilidad en los activos y procesos del negocio. Anexo 7.

Es necesario estimar la probabilidad realista de un incidente de seguridad sobre un activo a la vista de las amenazas y las vulnerabilidades dominantes, los impactos asociados a los activos y los controles de seguridad ya implementadas para proteger los activos.

4.1.4.3 Determinación del nivel de riesgo.

Para la realización de una estimación del riesgo, se requiere la asignación de valores a la posibilidad y a las consecuencias de un riesgo. Pueden ser cuantitativos o cualitativos.

Los análisis se basan en las consecuencias y posibilidad evaluadas. Anexo 8

Se puede considerar el costo beneficio, las inquietudes de las partes interesadas y otras variables, apropiadas para la evaluación del riesgo.

4.1.5 Evaluación del riesgo.

En base a los resultados del análisis y la finalidad de la evaluación del riesgo ayudará a la toma de decisiones, determinando los riesgos a tratar y la prioridad para implementar el tratamiento.

Esta etapa implica comparar el nivel de riesgo encontrado durante el proceso de análisis con los criterios de riesgo establecidos cuando se consideró el contexto.

En base a esta comparación se considera la necesidad del tratamiento.

Los criterios de evaluación utilizados para tomar decisiones deberían ser compatibles con el contexto para la gestión de riesgos externos e internos, teniendo en cuenta los objetivos de la institución y las opiniones de las partes interesadas. Anexo 9.

4.1.6 Costo económico.

La DGI, en los últimos años y como parte de su plan estratégico, ha ido aumentando la adquisición y explotación de la infraestructura tecnológica de la información y de comunicación (TIC´s).

Este hecho también ha obligado a la DGI, a incrementar los medios y medidas de seguridad para la protección de los datos almacenados y que igualmente se transmiten en los diferentes servicios que presta a nivel nacional.

Esa protección de los datos se ha materializado garantizando lo siguiente:

- La confidencialidad de la información, logrando que la información solamente sea accesible a las personas autorizadas;
- La integridad de la información, salvaguardando la veracidad y amplitud de la información y métodos de procesamiento;
- La disponibilidad de información, asegurando que los usuarios autorizados tienen acceso a la información y activos asociados cuando lo necesiten.

El alcance de los servicios electrónicos en la población fiscal se refleja en los siguientes datos porcentuales:

- Cubre hasta un 99.6% en declaraciones tributarias en línea.
- Emiten el 99% de las solvencias fiscales electrónicas.

- Recauda el 94% de los ingresos, por medio de pago en línea, lo que ha permitido incrementar gradualmente, el cumplimiento de las metas anuales de recaudaciones. (DGI, Nicaragua, 2016)

La discontinuidad de los servicios es el principal riesgo de la institución debido a que dejaría de cumplir con lo proyectado y los objetivos principales de la institución.

En base a los planes de tratamiento y eliminación del riesgo los costó económicos en que incurre la institución serán catalogados dependiendo del tipo acciones a tomar.

CAPITULO V – TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION

5.1 Descripción general del tratamiento del riesgo

El tratamiento dentro de la institución implica, la selección y la implementación de una o varias opciones para ser modificados.

Una vez realizada la implementación, los tratamientos proporcionan o modifican los controles.

El tratamiento del riesgo supone un proceso cíclico de:

- ✓ Valorar el tratamiento;
- ✓ Decidir si los niveles residuales son tolerables;
- ✓ Si no son tolerables, generar un nuevo tratamiento; y
- ✓ Evaluar la eficacia de este tratamiento.

5.2 Opciones del tratamiento del riesgo

Las opciones de tratamiento del riesgo no se excluyen necesariamente unas a otras, ni son apropiadas en todas las circunstancias. Las opciones pueden incluir lo siguiente:

a) Evitar el riesgo decidiendo no iniciar o no continuar con la actividad que lo causa.
b) Aceptarlo o aumentar a fin de perseguir una oportunidad;
c) Eliminar la fuente;
d) Modificar la probabilidad;
e) Modificar las consecuencias;

f) Compartirlo con otras partes (incluyendo los contratos y el financiamiento del riesgo); y

g) Mantenerlo en base a una decisión informada.

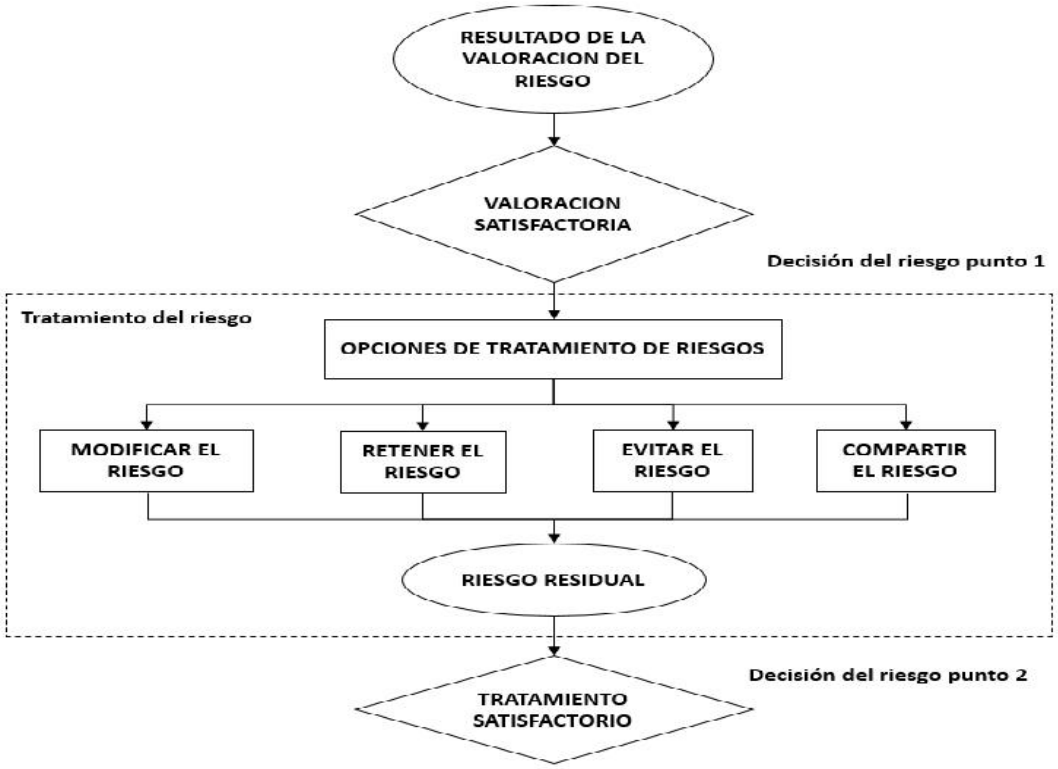
Al seleccionar opciones de tratamiento del riesgo, la institución deberá tener en consideración los valores y las percepciones de las partes interesadas y los medios apropiados para comunicarse con ellas.

El plan de tratamiento debe identificar claramente el orden de prioridad que puede constituir un riesgo importante. Para tener la seguridad de que las medidas son eficaces, es necesario que el seguimiento sea una parte integrante del plan de tratamiento de riesgo.

El tratamiento del riesgo puede introducir riesgos secundarios que necesitan que se aprecien, se traten, se realice seguimiento y se revisen. Estos riesgos secundarios deberán de incorporarse en el mismo plan de tratamiento que el riesgo original, y no tratarse como riesgo nuevo. La relación entre los dos riesgos debería identificarse y mantenerse.

La actividad del tratamiento dentro del proceso de gestión de riesgo de la seguridad de la información se muestra en la siguiente imagen.

Ilustración 2 Actividad de tratamiento del riesgo (ISO 27005:2011)



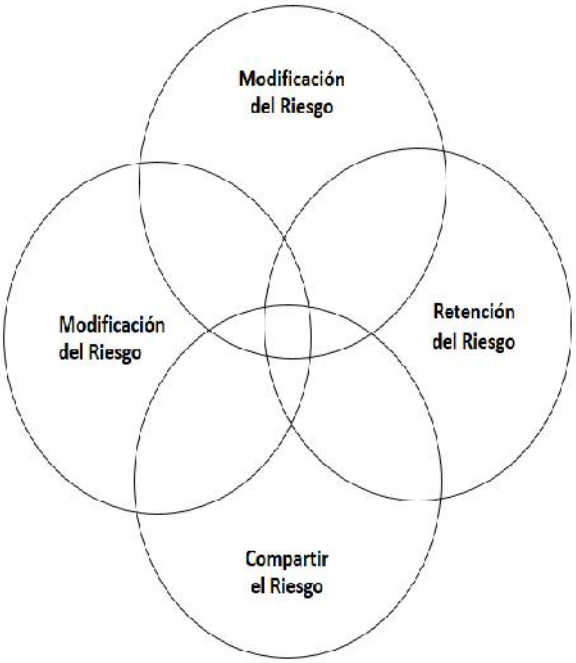
Las opciones de tratamiento del riesgo deberán ser seleccionadas sobre la base de los resultados de la evaluación, el coste esperado de la aplicación de estas opciones y los beneficios esperados de las mismas.

Cuando se pueden obtener grandes reducciones en los riesgos son relativamente bajo nivel de gastos, se deberían aplicar tales opciones. Otras iniciativas para las mejoras pueden no ser rentables y debe ser ejercido el sano juicio en decidir si son justificable o no.

De manera general las consecuencias negativas deberían ser tan bajas como sea posible. Independientemente de los criterios absolutos.

El método de apreciación del riesgo debería permitir la gestión del riesgo de acuerdo a las opciones según ilustración 2.

Ilustración 3 Las Opciones de Tratamiento del Riesgo (ISO 27005, clausula 9)



Modificación del Riesgo
Presentar, retirar o modificar los controles de modo que el riesgo residual puede ser evaluado como aceptable

Retención del Riesgo
La dirección decidió aceptar el nivel real de riesgo

Evitar el Riesgo
Cancelación o modificación de una actividad o conjunto de actividades relacionadas con riesgos

Compartir el Riesgo
Decisión de compartir riesgos con las partes externas: pólizas de seguros o tercerización.

Las consecuencias negativas de los riesgos deberían ser tan bajas como sea razonablemente posible, independientemente de los criterios absolutos. Los administradores deben considerar los riesgos que son comunes, pero graves. En tales casos, se deben llevar a cabo controles que no están justificados por motivos estrictamente económicos.

Las opciones mencionadas anteriormente en la ilustración 3 para el tratamiento del riesgo no son mutuamente excluyentes. Algunas veces la institución se puede beneficiar sustancialmente, mediante una combinación de opciones, tales como reducir la posibilidad del riesgo, reducir sus consecuencias y compartir o retener cualquier riesgo residual.

Algunos tratamientos del riesgo pueden efectivamente tratar más de uno, pueden ser incorporados la toma de conciencia y formación en la seguridad de la información.

La identificación de controles existentes es un elemento importante dentro del tratamiento del riesgo ya que puede determinar que estos excedan las necesidades actuales, en términos de comparaciones de costos, incluyendo el mantenimiento.

Las opciones de tratamiento del riesgo se deberán considerar tomando en cuenta: como se percibe por las partes afectadas y las maneras más apropiadas para comunicarse con esas partes.

5.2.1 Modificación del riesgo.

En la modificación del riesgo es necesario gestionarlo por medio de introducción, supresión o alteración de los controles, de manera que el riesgo residual se pueda revalorar como aceptable.

Se debe tomar controles apropiados y justificados para cumplir los requisitos identificados mediante la valoración del riesgo y el tratamiento del mismo. Es necesario tomar en cuenta todos aquellos requisitos legales, reglamentarios o contractuales.

Existen muchas restricciones que puede afectar la selección de controles como: requisitos de desempeño, capacidad de gestión (requisitos de soporte operacional) y problemas de compatibilidad los cuales pueden obstaculizar el uso de ciertos controles o podrían inducir error humano ya sea, anulando el control, dando falso sentido de seguridad o incrementando el riesgo más allá de no tener el control.

Se deben de tomar en cuenta diversas restricciones al seleccionar controles. Típicamente se consideran:

- Restricciones de tiempo.

- Restricciones financieras.
- Restricciones técnicas.
- Restricciones operacionales.
- Restricciones culturales.
- Restricciones éticas.
- Restricciones ambientales.
- Restricciones legales.
- Restricciones de uso.
- Restricciones de personal.
- Restricciones para la integración de controles nuevos y existentes.

En base a las políticas institucional la DGI, gestiona los controles y procesos de cambios a través de Disposiciones Administrativas Internas aprobadas por la instancia superior.

5.2.1.1 Restricciones para la modificación del riesgo.

5.2.1.1.1 Restricciones de tiempo.

Es necesario establecer parámetros o tiempo estipulado dependiendo del proceso como, por ejemplo:

- ✓ Se deberá de ejecutar durante un periodo de tiempo aceptable para la dirección de la institución.
- ✓ La ejecución de un control se debe realizar dentro del tiempo de vida de la información o del sistema.
- ✓ El tiempo que la institución puede estar expuesto a un riesgo en particular.

5.2.1.1.2 Restricciones financieras.

Los controles a implementar no deben tener costo elevado que el valor de los riesgos a proteger, excepto cuando el cumplimiento sea obligatorio (por obligación).

En este tipo de restricción es necesario tomar en cuenta que no se debe exceder los presupuestos asignados y poder alcanzar ventajas financieras a través de la utilización de controles. En algunos no se podrá alcanzar la seguridad deseada y el nivel de aceptación del riesgo, debido a las restricciones presupuestarias. Esto último ya deberá ser decisión de la dirección de la institución.

Cabe mencionar que los presupuestos establecidos para los controles se deberán de utilizar como un factor limitante solo si se tiene cuidado considerable.

5.2.1.1.3 Restricciones técnicas.

En esta restricción es importante tomar en cuenta aquellos elementos retrospectivos de controles a un proceso o sistema existente a menudo se dificulta por restricciones técnicas. Estas dificultades pueden mover los controles hacia los aspectos físicos y de procedimiento de la seguridad. Puede que sea necesario revisar el plan de la seguridad de la información a fin de alcanzar los objetivos de seguridad. Esto puede ocurrir cuando los controles no cumplen los resultados esperados, en cuenta a reducción de riesgos sin pérdida de productividad.

5.2.1.1.4 Restricciones operacionales.

Se recomienda ser incorporadas desde el diseño de la implementación, con el objetivo de no incurrir en costos y complejidad de los controles.

5.2.1.1.5 Restricciones culturales.

Este tipo de aspecto no debe ser ignorado dentro de los controles, debido a que dependen del soporte activo del equipo técnico. Si este no entiende la necesidad del control o no lo encuentra culturalmente aceptable, el control se volverá inefectivo con el paso del tiempo.

5.2.1.1.6 Restricciones éticas.

Posee mayor implicación en los controles, ya que en su totalidad están basados en normas sociales. Estos pueden evitar la implementación de controles. La privacidad de la información puede cambiar dependiendo de la ética del país o del gobierno y sobre todo limitantes dentro de la institución.

5.2.1.1.7 Restricciones ambientales.

Definir los factores ambientales que afectan dentro de la institución, como, disponibilidad de espacio, condiciones climáticas extremas, geografía urbana y natural del entorno puede influir en la selección de controles, hay que valorar todos aquellos fenómenos naturales que afectarían la operatividad.

5.2.1.1.8 Restricciones legales.

Abordar la protección de datos personales o las disposiciones para el procesamiento de la información esto debido a que puede afectar la selección de controles. El cumplimiento legislativo o regulatorio puede incidir en ciertos tipos de controles incluyendo protección de datos y auditorías.

5.2.1.1.9 Restricciones de uso.

Es necesario proporcionar los controles con facilidad óptima de uso mientras alcanzan un nivel aceptable de riesgo residual para la institución. Los controles que son difícil de utilizar impactaran su efectividad, ya que los usuarios pueden tratar de evadirlo ignorarlo tanto como sea posible. Aquellos controles que sean complejos dentro de la institución podrían alentar los usuarios a encontrar métodos de accesos alternos no autorizados.

5.2.1.1.10 Restricciones de personal.

Se debe de considerar un conjunto de habilidades especializadas para implementar controles. La experiencia no puede estar disponible inmediatamente para la implementación de controles planificados o esta podría ser excesivamente costosa para la institución.

Aquí juegan un rol importante los equipos de trabajo, la forma que se coordinan y el trato que existe entre ellos, siendo un elemento negativo la discriminación ya que podría causar implicaciones para las políticas y prácticas de seguridad.

5.2.1.1.11 Restricciones de la integración de controles nuevos y existentes.

Los nuevos controles pueden no ser fácilmente implementados si hay incongruencia o incompatibilidad con los existentes. En este aspecto es muy importante el costo de cambio de controles a partir de los ya existentes a los planificados, debería de incluir los elementos a ser agregados a los costos globales de tratamiento del riesgo. Puede no ser posible implementarlo un debido a interferencia con los controles actuales.

5.2.2 Retención del riesgo.

Esta es una opción viable para la institución para diferentes escenarios. También, tenemos que aceptar los escenarios de riesgo a los que no podemos poner una precaución de seguridad y que no son asegurables.

Cuando el riesgo es aceptado, las partes interesadas deben ser informadas y aceptarlo.

Cabe mencionar que, si el nivel de riesgo cumple con los criterios de aceptación, no es necesario poner en marcha controles de seguridad adicionales y este puede ser aceptado de hecho.

Según la norma (INTECO, 2014), apartado 4.2.1, f), 2) “aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfaga claramente la política y los criterios de la organización para la aceptación de riesgos”, describe la misma actividad.

5.2.3 Evitar el riesgo.

Si existen escenarios de riesgos identificados se consideran demasiado altos, se puede tomar una decisión para evitarlo:

- ✓ Mediante la cancelación de una actividad o conjunto de actividades
- ✓ modificando las condiciones en las que funciona la institución

La única manera de poder eliminar o evitar el riesgo por completo es eliminarlo en su fuente: Si se trata de una actividad que presenta un riesgo, la actividad no continuara.

Desde el punto de vista de los responsables de la toma de decisiones, esta estrategia es simple, la menos arriesgada y menos costosa, pero puede ser un obstáculo para el desarrollo de la organización.

Una situación en la que los riesgos son desconocidos o incontrolables, puede ser conveniente tratar de evitarlo temporalmente, tomar el tiempo necesario para analizar la situación y poner en práctica un plan para una adecuada gestión de riesgos.

La prevención del riesgo siempre debe de estar en equilibrio con las necesidades de negocio y las necesidades de seguridad de la institución.

5.2.4 Compartir el riesgo.

Al compartir el riesgo, la institución lo transfiere en su totalidad o en parte a un tercero.

Distribuirlo implica la decisión de transferir algunos a las partes externas. Compartir el riesgo puede crear nuevos escenarios o modificar los existentes.

Cabe mencionar que incluso si es posible compartir la gestión de un riesgo, normalmente no es posible compartir la responsabilidad sobre este riesgo. Las partes interesadas de la institución en general asigna la responsabilidad de un incidente o desastre a la institución.

Es necesario tomar en cuenta que siempre existe un riesgo residual relacionado con el reparto de este. En estos casos las aseguradoras, los contratos y las negociaciones se vuelven complejas para determinar el nivel de riesgo compartido, ya que el valor del riesgo residual es una consecuencia directa de ellos. En el caso de subcontratación, los

contratos pueden contener también exclusiones y más importante, algunos riesgos no se pueden compartir.

Los mecanismos de transferencia deben ser formalizados a través de acuerdo contractual.

5.3 Plan de tratamiento de riesgo

La finalidad del plan de tratamiento de riesgo dentro de la institución consiste en documentar la manera en que se implantarán las opciones de procedimientos elegidos. La información proporcionada en los planes de tratamiento debería incluir lo siguiente:

- Razones que justifica la selección de las opciones de tratamiento, se incluyen los beneficios conocidos.
- El personal responsable de la aprobación e implementación del plan.
- Las acciones propuestas.
- Las necesidades de recursos, incluyendo las contingencias.
- Las medidas del desempeño y las restricciones
- Los requisitos en materia de información y de seguimiento
- Calendario y la programación.

El plan de tratamiento debe formar parte e integrarse en los procesos de gestión de la institución y ser abordada con las partes interesadas.

Las personas que toman las decisiones y las otras partes interesadas deberán estar informadas de la naturaleza y amplitud del riesgo residual después del tratamiento del

riesgo. El riesgo residual deberá documentar y someter a seguimiento, revisión y cuando sea apropiado, a tratamiento adicional.

Las acciones prioritarias se determinan a fin de garantizar que las actividades se centren en el mayor riesgo, aunque otros procesos puedan influir en las prioridades de la política, como la necesidad de mostrar resultados a las altas direcciones de la institución o para obtener beneficios altos.

Una vez que han sido tomadas las decisiones sobre las opciones de tratamiento del riesgo, deben ser identificadas y planificadas las actividades para la aplicación de esas decisiones.

Las actividades deberían ser clasificadas en orden de prioridad y deben destinarse los recursos necesarios para el plan de tratamiento.

El plan de tratamiento es probable que adopte un enfoque más o menos elaborado, pero al menos debería aclarar los siguientes puntos:

- Las acciones a tomar
- Los recursos a asignar
- Las responsabilidades a tomar
- Las prioridades a ser secuenciadas

5.3.1. Roles y responsabilidades en la gestión de riesgo

Para lograr una excelente gestión de riesgo depende en gran amera la participación de los directivos y funcionarios, es de gran importancia identificar los actores que participaran en la gestión:

- Direccion superior: aprobaran las directrices para la administración y gestión de riesgo dentro de la institución, son los encargados de fortalecer las políticas de administración.
- Oficina de seguridad de la información: genera la metodología para la administración del riesgo de la institución, encargada de coordinar, capacitar y dar el seguimiento respectivo para su aplicación.
- Líderes o responsable de los procesos: identifican, analizan, evalúan y valoran los riesgos de la institución, periódicamente o cuando sea de suma urgencia, apoyan la ejecución de las diferentes etapas de la gestión de riesgo, significa que los procesos de la gestión están bajo su responsabilidad. Encargados de establecer las estrategias y responsabilidades para tratarlos.
- Funcionarios: son los encargados de ejecutar los controles y acciones definidas para la gestión de riesgo, son los que aportan la identificación de posibles riesgos que puedan afectar los objetivos y/o procesos de la institución.

CAPITULO VI – CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

La Dirección General de Ingresos, ha venido desarrollando planes estratégicos en temas de seguridad de la información, para el cumplimiento de sus objetivos institucionales, fortaleciendo controles en sus procesos, para garantizar la confidencialidad, disponibilidad e integridad de los datos y servicios en línea que brinda a los contribuyentes.

Dentro de los beneficios del uso del estándar ISO 27005, podemos destacar la estructuración de un proceso, controlar cada una de las actividades definidas, la eficiencia de los resultados, responsabilidades y validación e identificación de las mejoras.

Con la propuesta de gestión de riesgos de seguridad de la información, se podrá conocer y tener debidamente identificados los activos de información y la importancia que tienen dentro de los servicios brindados. Tomando en cuenta que una de las etapas de mucha importancia dentro del proceso de la gestión es crear conciencia y sensibilizar al personal en la cultura de los riesgos. Para que sean ellos mismos quienes puedan controlar y evaluar sus procesos.

Los factores externos e internos, ayudaran a identificar los riesgos, amenazas y vulnerabilidades latentes dentro de la institución Anexo 10, proyectando siempre un tratamiento de mejoramiento y evaluación del control interno, de esta manera se garantizará el cumplimiento institucional.

Es importante para el cumplimiento en todo el proceso de la gestión de riesgo, el apoyo gerencial en la asignación de recursos financiero y crear capacidades especializadas en el recurso humanos, así como las aprobaciones o cambios que se pueda llevar dentro de los procesos.

6.2 Recomendaciones

- Creación de una política de gestión de riesgo de seguridad de la información, con el objetivo de garantizar la aplicación de los procesos de control interno institucionales, para el efectivo cumplimiento de los objetivos estratégicos, de esta manera proteger los activos de información institucional, en contra de todas las amenazas y vulnerabilidad internas y externas, que se produzcan ya sea de forma deliberada como accidental.
- En base al Sistema de Gestión de Seguridad de la Informacion, orientar la seguridad y riesgos de la información como una responsabilidad de cada área a cargo de procesos críticos y de apoyo, tecnológicos y administrativos.
- Seguir priorizando la tecnología como el medio estratégico utilizado, para gestionar de manera rápida, eficiente y oportuna los procesos y las fuentes de información relacionada a la entrega y disponibilidad de servicios.
- Involucrar a todo el personal de las áreas sustantivas y capacitarlos, de esta manera comprometerlos al uso y gestión de riesgo, así como la concientización y la evaluación del grado de compromiso.
- Realizar evaluaciones periódicas de riesgo que permita a la Direccion General de Ingresos definir su apetito de riesgo de forma efectiva.

REFERENCIAS BIBLIOGRAFICAS

Computerworld FROM IDG. (18 de Marzo de 2010). *Computerworld* . Obtenido de http://www.computerworld.es/archive/de-la-teoria-a-la-practica-en-el-gobierno-ti

CORTES, Y. A. (2015). *Metodología de Gestión de Incidentes de Seguridad de la Información y Gestión de Riesgos para la Plataforma SIEM de una Entidad Financiera Basada en la Norma ISO/IEC 27035 E ISO/IEC 27005.* Bogota D.C.

Direccion General de Ingresos. (12 de Diciembre de 2016). *dgi.gob.ni*. Obtenido de dgi.gob.ni: https://www.dgi.gob.ni/pdfInfo/PlanEstrategico

GERENS. (28 de Diciembre de 2017). *GERENS*. Obtenido de https://gerens.pe/blog/gestion-riesgo-que-por-que-como/

Instituto Nacional de Ciberseguridad. (2015). *Gestion de riesgos una guia de aproximacion para el empresario.* España: Portales INCIBE.

INTECO. (2012). *Tecnología de información – Técnicas de seguridad – Gestión del Riesgo de la Seguridad de la Información.* Costa Rica.

INTECO. (2014). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información.* Costa Rica.

ISOTools Excellence. (6 de Mayo de 2015). *Blog Especializado en Sistemas de Gestión y Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

ISOTools Excellence. (5 de Enero de 2017). *Blog Especializado en Sistemas de Gestión y Seguridad de la Informacion*. Obtenido de https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

ISOTools Excellence. (15 de Junio de 2017). *Blog Especializado en Sistemas de Gestión y Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2017/06/iso-27005-gestion-del-riesgo-tecnologico/

ISOTools Excellence. (2018). La Clave del Exito para la Gestión de Riesgos. *ISOTools Excellence*, 8.

PECB. (2015). Gerente de Riesgos . En PECB, *Gerente de Riesgos* .

SIBOIF. (19 de Septiembre de 2007). *Lesgislacion Asamblea Nicaragua*. Obtenido de http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/7864260A19C7C67D062575B600601651?OpenDocument

Silva, J. (24 de Septiembre de 2017). *José Silva Correduria de Seguro S.L*. Obtenido de http://www.josilva.com/blog/Posts/show/importancia-de-la-gestion-de-riesgos-734

Z., R. A. (2011). Gestión de Riesgos tecnológicos basada en ISO 3100 e ISO 27005 y su aporte a la continuidad de negocios. *Articulo de Investigacion*, 56-66.

ANEXOS

Anexo 1

Causas	Riesgos	Consecuencia	Clasificación	Identificación del Riesgo
Medios o circunstancia	Evento que generara un impacto	Resultado que se pueden presentar	De acuerdo a su característica	Resultado esperado
Descripción a adecuada de los Riesgos				

Anexo 2

Criterio y caracteristica de activos										
ID Activo	Activo	Propietario	ubicación	Amenaza	Vulnerabilidad	Impacto			Probabilidad	Riesgo
						C	I	A		
DGI-001-2019	SERVIDOR PRODUCCION	JUAN PEREZ	CENTRO DE DATOS	VIRUS	ANTIVIRUS DEBIL	2	3	1	1	3
DGI-002-2019	SERVIDOR DE ARCHIVO	MIGUEL HERNANDEZ	CENTRO DE DATOS	VIRUS	ANTIVIRUS DEBIL	3	3	3	1	4
DGI-003-2019	CONTRATOS PROVEEDORES	JUAN PEREZ	ADQUISICION	DIVULGAR	ACCESO NO CONTROLADO	4	4	1	2	5
DGI-004-2019	PORTATIL	MILTON MARTINEZ	FINANZAS	ROBO	FALTA DE SEGURIDAD	5	4	3	2	6

Anexo 3

Criterios de clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Información pública reservada	Alta (A)	Alta (1)
Información pública clasificada	Media (M)	Media (2)
Información pública	Baja (B)	Baja (3)

Niveles de clasificación

Alta	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad y disponibilidad) es alta.
Media	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
Baja	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Anexo 4

La tabla siguiente muestra ejemplos de amenazas. La lista se puede utilizar durante el proceso de evaluación de la amenaza, las que pueden ser deliberadas, accidentales o ambientales (naturales) y pueden resultar, por ejemplo, en daño o pérdida de servicios esenciales.

Tipo de amenaza, donde:

D (Deliberada); se utilizada para toda acción deliberada que apunte a los activos de información.

A (Accidental); se utiliza para toda acción humana que accidentalmente puede dañar activos de información.

E (Ambiental); se utiliza para todos los accidentes que no se basen en acciones humana.

Tipo	Amenaza	Origen
Daños físicos	Fuego	A,D,E
	Daño por agua	A,D,E
	Contaminación	A,D,E
	Accidente mayor	A,D,E
	Destrucción de equipo o medios	A,D,E
	Polvo, corrosión, congelamiento	A,D,E
Eventos naturales	Fenómeno climático	E
	Fenómeno sísmico	E
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
	Inundación	E
Perdida de servicios esenciales	Falla de aire acondicionado o del sistema de suministro de agua	A,D
	Perdida de suministro de energía	A,D,E
	Falla del equipo de telecomunicaciones	A,D
Perturbación por la radiación	Radiación electromagnética	A,D,E
	Radiación térmica	A,D,E
	Pulsos electromagnéticos	A,D,E
Compromiso de información	Intercepción e interferencia de señales	D
	Espionaje remoto	D
	Escucha secreta	D
	Robo de medios o de documentos	D
	Robo de equipos	D
	Recuperación de medios reciclados o descartados	D
	Divulgación	A,D
	Datos de fuentes poco confiables	A,D
	Manipulación con hardware	D
	Manipulación con software	A,D
	Detección de posición	D
Fallas técnicas	Falla de equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A,D
	Mal funcionamiento del software	A
	Ruptura del mantenimiento del sistema de información	A,D
Acciones no autorizadas	Uso no autorizado del equipo	D

	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A,D
	Corrupción de datos	D
	Procesamiento ilegal de datos	D
Compromiso de funciones	Error de uso	A
	Abuso de derechos	A,D
	Falsificación de derechos	D
	Denegación de acciones	D
	No disponibilidad de personal	A,D,E

Fuentes de amenazas humanas

Fuente de amenaza	Motivación	Posibles consecuencias
Hacker, Cracker	Desafío Ego Rebelión Estatus Dinero	- Hacking - Ingeniera social - Intrusión o interrupción de Sistemas - Acceso no autorizado al sistema
Delito informático	Destrucción de información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de datos	- Delito informático (por ejemplo, acoso cibernético) - Acto fraudulento (por ejemplo, reproducción , suplantación de datos, intercepción) - Suplantación (Spoofing) - Intrusión en los sistemas
Terrorista	Chantaje Destrucción Explotación Venganza Beneficio político Cobertura mediática	- Bomba/Terrorismo - Guerra de información - Ataque de sistemas (por ejemplo, denegación distribuida de servicio) - Penetración de sistemas - Manipulación de sistemas
Espionaje industrial (inteligencia compañías, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	- Ventaja defensiva - Ventaja política - Explotación económica - Robo de información - Intrusión en la privacidad personal - Ingeniería social - Penetración de sistemas - Acceso no autorizado a sistemas (acceso a información clasificada, propietaria, y/o relacionada con tecnología)

Personal interno (empleados pobremente formados, descontentos, maliciosos, negligentes, deshonesto o despedidos)	Curiosidad Ego Inteligencia Ganancia económica Venganza Errores y omisiones no intencionales (por ejemplo, error de entrada de datos, error de programación)	- Asalto a un empleado - Chantaje - Observación de información empresarial - Mal uso de la computadora - Fraude y robo - Soborno de información - Entrada de datos falsificados o corruptos - Interceptación - Código malicioso (por ejemplo, virus, bomba, lógica, caballo de Troya) - Venta de información personal - Errores de sistemas - Intrusión de sistemas - Sabotaje de sistemas - Acceso no autorizado a sistemas

Anexo 5

A.5 Políticas de seguridad de la información	
A.5.1 Direccion de la gestión para la seguridad de la información	
Objetivo: Proporcionar dirección de la gestión y soporte para la seguridad de la información, de acuerdo con los requisitos del negocio y con la regulaciones y leyes pertinentes.	
A.5.1.1	Políticas para la seguridad de la información
A.5.1.2	Revisión de las políticas para la seguridad de la información
A.6. Organización de la seguridad de la información	
A.6.1 Organización interna	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	
A.6.1 Organización Interna	
A.6.1.1	Roles y responsabilidades de seguridad de la información.
A.6.1.2	Segregación de funciones
A.6.1.3	Contacto con autoridades
A.6.1.4	Contacto con grupo de interés especial
A.6.1.5	Seguridad de la información en gestión de proyectos
A.6.2 Dispositivos móviles y teletrabajo	
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivo móviles.	
A.6.2.1	Política de dispositivo móvil
A.6.2.2	Teletrabajo
A.7 Seguridad ligada a los recursos humanos	
A.7.1 Previo al empleo	
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados.	
A.7.1.1	Investigación
A.7.1.2	Términos y condiciones del empleo

A.7.2 Durante el empleo	
Objetivo: asegurar que los empleados y contratistas sean consciente sean consciente y cumplan con sus responsabilidad de seguridad de la información.	
A.7.2.1	Responsabilidad de la dirección
A.7.2.2	Toma de conciencia, educación y formación en seguridad de la información
A.7.2.3	Proceso disciplinario
A.7.3 Finalización o cambio de empleo	
Objetivo: proteger los intereses de la organización como parte del proceso de finalización o cambio de empleo.	
A.7.3.1	Finalización o cambio de empleo
A.8. Gestión de activos	
A.8.1 Responsabilidad por los activos	
Objetivo: Identificar los activos de la organización y definir las responsabilidades para la apropiada protección.	
A.8.1.1	Inventario de activos
A.8.1.2	Propiedad de los activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	Devoluciones de activos
A.8.2 Clasificación de la información	
Objetivo: Asegurar que la información recibe un nivel de protección apropiado, de acuerdo con su importancia para la organización.	
A.8.2.1	Clasificación de la información
A.8.2.2	Etiquetado de la información
A.8.2.3	Manejo de los activos
A.8.3 Manejo de los medios	
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de la información almacenada en los medios.	
A.8.3.1	Gestión de medios removibles
A.8.3.2	Eliminación de medios
A.8.3.3	Traslado de medios físicos
A.9 Control de acceso	
A.9.1 Requisitos del negocio para el control de acceso	
Objetivo: Limitar el acceso a la información y a los recursos de procesamiento de la información.	
A.9.1.1	Política de control de acceso
A.9.1.2	Acceso a redes y servicio de red
A.9.2 Gestión del acceso de usuarios	
Objetivos: Asegurar el acceso autorizado de los usuarios y evitar el acceso no autorizado a los sistemas y servicios.	
A.9.2.1	Registro y cancelación de registro de usuarios
A.9.2.2	Aprovisionamiento de acceso a usuarios
A.9.2.3	Gestión de derechos de acceso privilegiados
A.9.2.4	Gestión de la información secreta de autenticación de usuarios
A.9.2.5	Revisión de los derechos de acceso de los usuarios
A.9.2.6	Eliminación o ajuste de los derechos de acceso
A.9.3 Responsabilidades de los usuarios	

Objetivo: Hacer responsables a los usuarios de salvaguardar su información de autenticación.	
A.9.3.1	Uso de la información secreta de autenticación
A.9.4 Control de acceso no autorizado a los sistemas y aplicaciones.	
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.	
A.9.4.1	Restricción de acceso a la información
A.9.4.2	Procedimientos de acceso (log-on) seguros
A.9.4.3	Sistemas de gestión de contraseñas
A.9.4.4	Uso de programas utilitarios privilegiados
A.9.4.5	Control de acceso al código fuente de programas
A.10 Criptografía	
A.10.1 Controles de criptografía	
Objetivo: Asegurar del uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información.	
A.10.1.1	Política sobre el uso de controles criptográficos
A.10.1.2	Gestión de llaves
A.11 Seguridad física y ambiental	
A.11.1 Áreas segura	
Objetivo: Prevenir el acceso físico no autorizado, daños e interferencia a la información y a los recursos de procesamiento de la información de la organización.	
A.11.1.1	Perímetro de seguridad física
A.11.1.2	Controles de entrada física
A.11.1.3	Aseguramiento de oficinas, salas e instalaciones
A.11.1.4	Protección contra amenazas externas y ambientales
A.11.1.5	Trabajando en áreas seguras
A.11.1.6	Áreas de entrega y carga
A.11.2 Equipo	
Objetivo: Prevenir la perdida, daño, robo o compromiso de los archivos y la interrupción de las operaciones de la organización.	
A.11.2.1	Colocación y protección del equipo
A.11.2.2	Servicios de soporte
A.11.2.3	Seguridad del cableado
A.11.2.4	Mantenimiento del equipo
A.11.2.5	Remoción de activos
A.11.2.6	Seguridad del equipo y los activos fuera de las instalaciones
A.11.2.7	Seguridad en la eliminación o reutilización del equipo
A.11.2.8	Equipo desatendido por el usuario
A.11.2.9	Política de pantalla
A.12 Seguridad de las operaciones	
A.12.1 Procedimientos y responsabilidades operacionales	
Objetivo: Asegurarse de las operaciones correctas y seguras de los recursos de procesamiento de la información.	
A.12.1.1	Procedimientos de operación documentados
A.12.1.2	Gestión de cambios
A.12.1.3	Gestión de la capacidad
A.12.1.4	Separación de ambientes de desarrollo, pruebas y operación
A.12.2. Protección contra código malicioso (malware)	

Objetivo: Asegurar que las instalaciones de procesamiento de información y la información están protegidas contra el código malicioso.	
A.12.2.1	Controles contra el código malicioso
A.12.3 Respaldo	
Objetivo: Proteger contra la perdida de datos	
A.12.3.1	Respaldo de la información
A.12.4 Registro y seguimiento	
Objetivo: Registrar los eventos y generar evidencia	
A.12.4.1	Registro de eventos
A.12.4.2	Protección del registro de información (log)
A.12.4.3	Registros del administrador y el operador
A.12.4.4	Sincronización de reloj
A.12.5 Control de software operativo	
Objetivo: Asegurar la integridad de los sistemas operativos.	
A.12.5.1	Instalación de software en los sistemas en operación
A.12.6 Gestión de vulnerabilidades técnicas	
Objetivo: Prevenir la explotación de vulnerabilidades técnicas.	
A.12.6.1	Gestión de vulnerabilidades técnicas
A.12.6.2	Restricciones en la instalación de software
A.12.7 Consideraciones de auditoria de sistemas de información	
Objetivo: Minimizar el impacto de las actividades de auditoria en los sistemas en operación.	
A.12.7.1	Controles de auditoria de sistemas de información
A.13 Seguridad de las comunicaciones	
A.13.1 Gestión de seguridad de la red	
Objetivo: Asegurar la protección de la información en las redes y sus recursos de soporte de procesamiento de información.	
A.13.1.1	Controles de red
A.13.1.2	Seguridad de los servicios de red
A.13.1.3	Segregación en las redes
A.13.2 Transferencia de información	
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	
A.13.2.1	Políticas y procedimientos de transferencia de información
A.13.2.2	Acuerdos de transferencia de información
A.13.2.3	Mensajería electrónica
A.13.2.4	Acuerdos de confidencialidad o no divulgación
A.14 Adquisición, desarrollo y mantenimiento de sistemas	
A.14.1 Requisitos de seguridad de sistemas de información	
Objetivo: Asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.	
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información
A.14.1.2	Asegurar los servicios de aplicaciones en las redes publicas
A.14.1.3	Protección de las transacciones de servicios de aplicación
A.14.2 Seguridad en los procesos de desarrollo y soporte	

Objetivo: Asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida del desarrollo de sistemas de información.	
A.14.2.1	Política de desarrollo seguro
A.14.2.2	Procedimientos de control de cambios
A.14.2.3	Revisión técnica de las aplicaciones después de realizar cambios de plataforma de operación.
A.14.2.4	Restricciones en los cambios a los paquetes de software
A.14.2.5	Principios de ingeniería de sistemas seguros
A.14.2.6	Ambiente de desarrollo seguro
A.14.2.7	Desarrollo contratado externamente
A.14.2.8	Pruebas de seguridad de sistemas
A.14.2.9	Pruebas de aceptación del sistema
A.14.3 Pruebas de datos	
Objetivo: Asegurar la protección de los datos utilizados para la prueba.	
A.14.3.1	Protección de los datos de prueba
A.15 Relaciones con los proveedores	
A.15.1 Seguridad de la información en la relación con los proveedores	
Objetivo: Asegurar la protección de los activos de la organización que son accesible por los proveedores.	
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores
A.15.1.2	Abordar la seguridad dentro de los acuerdos de proveedores
A.15.1.3	Cadena de suministro de tecnologías de información y comunicaciones.
A.15.2 Gestión de la entrega de servicios del proveedor	
A.15.2.1	Seguimiento y revisión de los servicios de proveedores
A.15.2.2	Gestión de cambios en los servicios de proveedores
A.16 Gestión de incidentes de seguridad de la información	
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información	
Objetivo: Asegurar que se aplique un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y debilidades de seguridad.	
A.16.1.1	Responsabilidades y procedimientos
A.16.1.2	Reporte de eventos de seguridad de la información
A.16.1.3	Reporte de debilidades de seguridad de la información
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información
A.16.1.6	Aprendiendo de los incidentes de seguridad de la información
A.16.1.7	Recolección de evidencia
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	
A.17.1 Continuidad de la seguridad de la información	
Objetivo: La continuidad de la seguridad de la información debe ser integrada en los sistemas de gestión de la continuidad de negocio de la organización.	
A.17.1.1	Planificación de la continuidad de seguridad de la información
A.17.1.2	Implementación de la continuidad de seguridad de la información
A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información.
A.17.2 Redundancias	

Objetivo: Asegurar la disponibilidad de los recursos de procesamiento de información	
A.17.2.1	Disponibilidad de recursos de procesamiento de información
A.18 Cumplimiento	
A.18.1 Cumplimiento de los requisitos legales y contractuales	
A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales
A.18.1.2	Derechos de propiedad intelectual
A.18.1.3	Protección de registros
A.18.1.4	Privacidad y protección de datos personales
A.18.1.5	Regulación de los controles criptográficos
A.18.2 Revisión de seguridad de la información	
Objetivo: Asegurar que la seguridad de la información sea implementada y opere de acuerdo con las políticas y procedimientos de la organización.	
A.18.2.1	Revisiones independientes de seguridad de la información
A.18.2.2	Cumplimiento con las políticas y normas de seguridad
A.18.2.3	Revisiones de cumplimiento técnico

Anexo 6

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
Degradación del rendimiento	Cambio accidental	Violación de la privacidad de los usuarios o clientes
Interrupción del servicio	Modificación deliberada	Violación de la privacidad del personal de la organización
Inaccesibilidad de los servicios	Resultados incorrectos	Divulgación de información confidencial
Interrupción de las operaciones	Resultados incompletos	
	Perdida de datos	

Anexo 7

Nivel	Escala Cualitativa	Probabilidad
0	Muy rara	Menos de una vez cada 100 años
1	Rara	Una vez cada 10 años en promedio
2	Posible	Una vez cada 3 años en promedio
3	Muy posible	Una vez al año en promedio
4	Probable	Varias veces al año
5	Casi Común	Varias veces por mes
6	Común	Varias veces por semana
7	Muy común	Varias veces por día

Anexo 8

Determinación del riesgo

	Muy baja probabilidad	Baja probabilidad	Probabilidad media	Alta probabilidad	Muy alta probabilidad
Muy bajo impacto	**0**	**1**	**2**	**3**	**4**
Bajo impacto	**1**	**2**	**3**	**4**	**5**
Mediano impacto	**2**	**3**	**4**	**5**	**6**
Alto impacto	**3**	**4**	**5**	**6**	**7**
Muy alto impacto	**4**	**5**	**6**	**7**	**8**

Anexo 9

Amenaza	Consecuencia (valor del activo)	Probabilidad de ocurrencia de la amenaza	Medida del riesgo	Clasificación de amenazas
Amenaza A				
Amenaza B				
Amenaza C				
Amenaza D				
Amenaza E				
Amenaza F				

Este es un procedimiento que permite que diferentes amenazas con diferentes consecuencias y posibilidad de ocurrencia se comparen y clasifiquen en orden de prioridad. En algunos casos va a ser necesario asociar valores monetarios con las escalas empíricas aquí utilizadas.

Anexo 10

Amenazas
Acceso a la red o al sistema de información por personas no autorizadas.
Amenaza o ataque con bomba.
Incumplimiento de relaciones contractuales.
Infracción legal.
Comprometer información confidencial.
Ocultar la identidad de un usuario.
Daño causado por un tercero.
Daños resultantes de las pruebas de penetración.
Destrucción de registros.
Desastre generado por causas humanas.
Desastre natural, incendio, inundación, rayo.
Revelación de información.
Divulgación de contraseñas.
Malversación y fraude.
Errores en mantenimiento.
Fallo de los enlaces de comunicación.
Falsificación de registros.
Espionaje industrial.
Fuga de información.
Interrupción de procesos de negocio.
Pérdida de electricidad.
Pérdida de servicios de apoyo.
Mal funcionamiento del equipo.
Código malicioso.
Uso indebido de los sistemas de información.
Uso indebido de las herramientas de auditoría.
Contaminación.
Errores de software.
Huelgas o paros.
Ataques terroristas.
Hurtos o vandalismo.
Cambio involuntario de datos en un sistema de información.
Cambios no autorizados de registros.
Instalación no autorizada de software.
Acceso físico no autorizado.
Uso no autorizado de material con copyright.
Uso no autorizado de software.
Error de usuario.

Vulnerabilidades
Interfaz de usuario complicada.
Contraseñas predeterminadas no modificadas.
Eliminación de medios de almacenamiento sin eliminar datos.
Sensibilidad del equipo a los cambios de voltaje.
Sensibilidad del equipo a la humedad, temperatura o contaminantes.
Inadecuada seguridad del cableado.
Inadecuada gestión de capacidad del sistema.
Gestión inadecuada del cambio.
Clasificación inadecuada de la información.
Control inadecuado del acceso físico.
Mantenimiento inadecuado.
Inadecuada gestión de red.
Respaldo inapropiado o irregular.
Inadecuada gestión y protección de contraseñas.
Protección física no apropiada.
Reemplazo inadecuado de equipos viejos.
Falta de formación y conciencia sobre seguridad.
Inadecuada segregación de funciones.
Mala segregación de las instalaciones operativas y de prueba.
Insuficiente supervisión de los empleados y vendedores.
Especificación incompleta para el desarrollo de software.
Pruebas de software insuficientes.
Falta de política de acceso o política de acceso remoto.
Ausencia de política de escritorio limpio y pantalla clara.
Falta de control sobre los datos de entrada y salida.
Falta de documentación interna.
Carencia o mala implementación de la auditoría interna.
Falta de políticas para el uso de la criptografía.
Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.
Desprotección en equipos móviles.
Falta de redundancia, copia única.
Ausencia de sistemas de identificación y autenticación.
No validación de los datos procesados.
Ubicación vulnerable a inundaciones.
Mala selección de datos de prueba.
Copia no controlada de datos.
Descarga no controlada de Internet.
Uso incontrolado de sistemas de información.
Software no documentado.
Empleados desmotivados.
Conexiones a red pública desprotegidas.
Los derechos del usuario no se revisan regularmente.