UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

MAESTRIA EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

TRABAJO DE GRADUACIÓN

METODOLOGÍA PARA EVALUAR Y GESTIONAR LOS RIESGOS EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA CÁMARA DE COMERCIO E INDUSTRIA DE EL SALVADOR, BASADA EN LA NORMA ISO 31000:2018 INCISOS DEL 6.4 AL 6.7, APLICANDO MAGERIT

PARA OPTAR AL GRADO DE

MASTER EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

MASTER LEONARDO JOSE CASTILLO PERLA

PRESENTADO POR:

Celenia Evelyn González de Alvarenga

Yanira Elizabeth Ascencio García

Mario Enrique Ascencio García

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Agosto 2018

AGRADECIMIENTOS

A Dios, por permitirme finalizar el presente proyecto, a mi madre por su paciencia, su apoyo incondicional y sus sabios consejos que sin ellos el camino sería más difícil, a mi esposo y mis grandes amores mis hijas e hijo los que son mi motivación y la razón por la que vale la pena vivir, a mis amigas y amigos que me expresaron su alegría por superar el presente desafío y a mis compañeros y amigos de tesis por acompañarme con su esfuerzo y dedicación en este proyecto.

Celenia Evelyn González de Alvarenga

Gracias al todo poderoso por permitirme concluir este proyecto, y a mi familia que me apoyo en todo momento, a los colegas de tesis por el valioso aporte a la conclusión de este proyecto, al asesor que nos ayudó de gran manera a en el proceso del desarrollo de la tesis.

Mario Enrique Ascencio García

Agradezco a Dios por haberme guiado y acompañado a lo largo de este proyecto, por ser en los momentos difíciles mi fortaleza y por brindarme la oportunidad de muchos aprendizajes durante la vida, a los catedráticos que compartieron sus conocimientos, a mis compañeros y colegas de tesis por su denuedo y compartir sus experiencias, a mi madre por ser mi apoyo incondicional en todo momento, a mi padre, mis hermanos y mi pareja por su apoyo.

Yanira Elizabeth Ascencio García

RESUMEN

En la actualidad las empresas administran información de sus procesos de negocio, dicha información independiente del medio de almacenamiento y trasmisión es considerada como el recurso de vital importancia para el éxito y la continuidad del servicio porque de ello depende la toma de decisiones y el conocimiento interno de la misma.

En un proceso de evaluación de riesgos en el que se identifican los responsables y sus funciones dentro del proceso, las políticas e instancias de aplicación control del mismo, además se tipifican los activos de información, las posibles amenazas, se valoran los activos, con el impacto y la determinación de los riesgos, lo que da paso a la gestión de los mismos con el objeto que de forma preventiva se tomen las medidas con el conocimiento del grado de afectación o se acepten los riesgos según el apetito establecido por la alta Dirección.

En el presente proyecto se desarrolla el proceso de evaluación de los riesgos de TI, finalizando con la aplicación de la metodología en el caso de uso del proceso de “Respaldo de datos”, debido a la preocupación del resguardo de la información de la organización, se ha tomado como referencia con el propósito que ayude a visualizar de forma más amplia la aplicación y la importancia de prevenir riesgos mediante la aplicación de un proceso de evaluación de los riesgos de TI, que se ha desarrollado sobre la base de los marcos de referencia como ISO/IEC 31000:2018, Magerit método para riesgos de TI y COBIT 5 .

INDICE

INTRODUCCIÓN

El aumento en la adquisición de elementos tecnológicos para el buen desempeño de sus procesos operativos y la necesidad de obtener respuestas inmediatas de información, relacionadas con el estado de los negocios, lleva inmerso nuevos riesgos, lo que crea nuevos desafíos que deben enfrentarse para alcanzar los objetivos y metas de las organizaciones.

Por esta razón las organizaciones se ven en la necesidad de gestionar los riesgos en la infraestructura tecnológica, debido a que el riesgo en los sistemas de información es un factor que debe ser evaluado, que si se concreta puede afectar el logro de los objetivos organizacionales.

La gestión de riesgos, debe ser parte importante y valiosa del gobierno y la gestión eficaz de la organización, por que aborda la incertidumbre de lo que puede suceder y la medición para tratar los efectos de un evento de riesgo.

CAPITULO I. PLANTEAMIENTO DEL PROBLEMA

1.1. IDENTIFICACIÓN DEL PROBLEMA

La Cámara de Comercio e Industria de El Salvador (CCIES) fue fundada el 31 de diciembre de 1915 por distinguidos empresarios de sólido prestigio del país.

La CCIES es una gremial empresarial no lucrativa constituida con fines de servicio y de conformidad con las leyes de la República.

La creación de la Cámara de Comercio fue motivada por la necesidad de organizar al sector privado a fin de reactivar la economía nacional, afectada en aquel entonces por la depresión económica ocasionada por la Primera Guerra Mundial.

La principal función de la Cámara de Comercio es la representatividad gremial y la defensa de principios y valores de libre empresa, siendo una gremial multisectorial entre los principales beneficios de pertenecer a la gremial están: talleres especializados, espacios comerciales, encuentros de negocios, apoyo y vinculación en las áreas legal, aduanas, comercio internacional, capacitación al capital humano y programas de formación para la alta gerencia, seguros colectivos de vida y médicos, etc.

Actualmente la CCIES, presenta los retos siguientes:

- Carece de una metodología de gestión del riesgo informático, implicando así, un alto grado de tolerancia a la pérdida de información, por la alta exposición a la pérdida de datos para la empresa.
- No existe un procedimiento el cual indique la forma adecuada de realizar la transferencia del conocimiento, por lo que al tener una rotación de personal en algún puesto no se transfiere ese conocimiento o si se realiza no se hace de forma sistematizada.
- El proceso de respaldo de los datos de equipos informáticos no encuentra sistematizado; situación obliga a realizarlo de manera manual, con una unidad de disco duro externo.
- Los respaldos de las bases de datos son realizados periódicamente, y por falta de espacio, se ejecuta un borrado de los respaldos de datos más antiguos.
- Adicionalmente, toda la información respaldada queda en la misma ubicación, por lo que, al suceder algún siniestro en el lugar, se corre el riesgo de perder en su totalidad la información, sin que exista una evaluación de riesgo a dicho suceso a efecto mitigar la pérdida de información.

En ese orden de ideas, se considera que la falta de una guía que proporcione a la CCIES, las directrices para identificar, valorar y gestionar los riesgos en la

infraestructura tecnológica, no permite a la alta Gerencia comprender que existen amenazas y vulnerabilidades que ponen en riesgo elementos críticos del entorno tecnológico y en consecuencia podrán amenazar el cumplimiento de los objetivos estratégicos de la organización.

1.2. DEFINICIÓN DEL PROBLEMA

La Cámara de Comercio e Industria de El Salvador, no cuenta con un proceso que le proporcione las directrices para identificar, valorar, medir, cuantificar y estimar el impacto de los eventos de riesgo y su gestión de los riesgos relacionados a la infraestructura tecnológica.

1.3. OBJETIVO GENERAL

Desarrollar una metodología para la gestión del riesgo, basados en el marco de referencia ISO 31000:2018.

1.4. OBJETIVOS ESPECÍFICOS

- Identificar para los principales procesos de tecnología, una matriz de responsabilidades RACI por sus siglas en inglés (Responsabile, Accountable, Consulted, informed), que en adelante se denominara como Matriz RACI, así como la valoración de los activos de información.

- Identificar y definir el apetito de Riesgo de la organización ante las amenazas y las vulnerabilidades sobre los activos de tecnología y el nivel de impacto de los riesgos.

- Determinar una lista de controles para la gestión del riesgo, de tal manera que la organización cuente con un conjunto de métodos sistematizados para enfrentar los riesgos y decidir aceptarlo, transferirlo, disminuirlo o evitarlo.

1.5. JUSTIFICACIÓN

Cuando una organización depende de herramientas tecnológicas para brindar servicios a sus usuarios y estos forman parte de su objetivo principal, se debe poner atención en los riesgos que podrían afectar la disponibilidad de dichas herramientas; y para lograrlo se requerirá de un proceso en la que se identifiquen los riesgos que le puedan afectar y lleven a un inadecuado funcionamiento hasta detener su funcionamiento ante los usuarios.

Es de alta importancia y de prioridad realizar un proceso en el que se definan los criterios para la identificación, valoración y la forma de gestionar los riesgos que afectan a la infraestructura tecnológica.

Este documento es un análisis básico que puede utilizarse como guía de valoración y gestión de los riesgos de tecnología a efecto de identificar de forma preventiva los riesgos relativos a la tecnología y tomar acciones de control con conocimiento de estos.

Al mismo tiempo de facilitar la identificarlas de las amenazas, el impacto de estas si llegan a materializarse y el riesgo al que se encuentran expuestos lo activos de la institución.

Con esta guía se pretende brindar, una herramienta, que le ayude a dar seguimiento al riesgo al que se encuentran expuestos los activos y de esta forma que la institución tome una decisión y defina cuál es el apetito de riesgo con el que se siente satisfecho de aceptar.

1.6. DELIMITACIÓN

Proponer una guía de implementación, para gestionar el riesgo en la infraestructura tecnológica de la CCIES, que permita realizar un diagnóstico mediante el análisis de brecha del estado deseado y estado actual, que proporcione una metodología para la administración del riesgo, ya sea que este se asuma, se transfiera o el grado en que este se mitigue, dándole un mayor grado de madurez a la empresa definiendo el estado deseado.

CAPITULO II. MARCO TEORICO

	NTS ISO 31000:2018	MAGERIT	COBIT 5
CONCEPTO	Norma de adopción idéntica (IDT) a la Norma ISO 31000:2018 “Gestión del riesgo-Directrices”,	Metodología de análisis de riesgos y gestión de riesgos derivado del uso de tecnología de la información,	COBIT 5 desarrollado por ISACA en 2012 integra los marcos de gobierno, control, auditoria y riesgo, es un marco de gestión y de negocio

	publicado por el Organismo Salvadoreño de Normalización (OSN), resultado del trabajo que el Grupo ISI/TC 262/STTF vienen desarrollando desde el año 2017.	elaborada por el Consejo Superior de Administración Electrónica (CSAE) y publicada por el Ministerio de Administración Pública de España, encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del Gobierno de España.	global para el gobierno y la gestión de las TI de la empresa.
CARACTERISTICAS	Para las personas que protegen el valor de las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando los objetivos de la organización. Considera que la gestión de riesgos se basa en principios, marco de referencia y procesos descritos, que podrían ser adaptados para que la gestión de riesgos sea eficiente, eficaz y coherente.	Proporciona a los responsables de la organización el conocimiento de la existencia de riesgos y la forma de gestionarlos, ofrece un método sistemático para analizar los riesgos derivados del uso de la tecnología y las comunicaciones, ayuda a descubrir y mantener los riesgos bajo control.	COBIT 5 une los cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información, así como su uso en beneficio de las partes interesadas, quienes impulsan a uno de sus objetivos que trata sobre la optimización de los riesgos.
FASES DE LA GESTIÓN DE RIESGOS	Identificación del riesgo: reconocer y describir los riesgos que pueden ayudar o limitar a una organización lograr sus objetivos. Análisis del Riesgo: comprender la naturaleza del riesgo	Análisis de riesgos: permite determinar cómo es, cuánto vale y como se encuentran protegidos los activos. Paso 1: Activos Paso 2: Amenazas, impacto y riesgo	Dominio de evaluar, orientar y supervisar. EDM03 Asegurar la optimización del riesgo, proceso para asegurar que el apetito y tolerancia al riesgo de la empresa son atendidos, articulados y comunicados y que el

	y sus características, debería considerar la probabilidad de los eventos y sus consecuencias, la naturaleza y magnitud de las consecuencias, la eficacia de los controles existentes. Valoración del riesgo: implica comparar los resultados del análisis del riesgo, con los criterios de riesgo establecidos para determinar, cuándo se requiere una acción adicional. Tratamientos del riesgo: consiste en seleccionar e implementar opciones para abordar el riesgo, e implica un proceso de seleccionar opciones para el tratamiento, implementar el tratamiento, evaluar la eficacia del tratamiento, decidir si el riesgo residual es aceptable, si no es efectuar tratamiento adicional. Registro e informe: sus resultados se deben documentar e informar.	potencial. Paso 3: Salvaguardas Paso 4 Impacto Residual Paso 5: Riesgo Residual Proceso de gestión: Evaluación e interpretación de los valores de impacto y riesgos residuales. Tratamiento del riesgo (aceptar, trasladar, mitigar, controlar) Comunicación, seguimiento y revisión.	riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado. Metas de TI y métricas relacionadas. Matriz RACI del proceso EDM03. Procesos de entrada, Salida y actividades. Dominio de Alinear, Planear y Organizar: APO12 Gestión de Riesgo, proceso de identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de los niveles de tolerancia establecida por la dirección ejecutiva de la empresa. Matriz RACI por sus siglas en ingles del proceso APO12 Todos los procesos incluyen prácticas y actividades que son diseñadas para tratar el riesgo relacionado (evitar, reducir / mitigar / controlar/ compartir / transferir / aceptar).
AMBITO DE APLICACIÓN	Proporciona un enfoque común para gestionar cualquier tipo de riesgo y no	Gobierno, compañías grandes comerciales y no comerciales, pymes	No es específico de una industria, gobierno, empresas o compañías grandes, comerciales o

	es específico de una industria o sector.		no comerciales.
VENTAJAS	Proporciona las directrices para la gestión de riesgos en general, permite adaptarlo a cualquier riesgo de la organización	Proporciona el método completo y aplica las directrices de evaluación de la ISO 31000, desde la identificación de los activos hasta la comunicación a las partes interesadas. Posee una base documental de apoyo al desarrollo de la gestión de riesgos de tecnología de la información.	Un marco de referencia integral, para las áreas claves de gobierno y gestión, que se conforma por cinco dominios: el primer dominio, evaluar, orientar y supervisar. El segundo dominio de alineación, planificación y organización. Un tercer dominio construir, adquirir e implementar. Un cuarto, entregar, dar servicio y soporte y el quinto dominio, supervisar, Evaluar y valorar.
DESVENTAJAS	No proporciona un método detallado, para gestionar los riesgos, únicamente las directrices generales.	No involucra las áreas del gobierno para gestionar el riesgo.	No es específico para gestionar los riesgos, involucra gestión de TI, estrategia, calidad, presupuesto, recurso humano entre otros.

Tabla 1. Comparación de los marcos teóricos

CAPITULO III. MARCOS DE REFERENCIA

1. MARCO DE REFERENCIA NTS ISO 31000:2018

La Norma técnica salvadoreña NTS ISO 31000:2018, ofrece las directrices y principios para gestionar el riesgo, publicada por el Organismo Salvadoreño de Normalización (OSN).
Dicha Norma establece que la gestión de riesgo se basa en los principios, marco de referencia y el proceso, que consisten en lo siguiente:

Los principios proporcionan orientación sobre las características de una gestión del riesgo eficaz y eficiente, en lo que respecta al desarrollo del marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo, de la misma forma el proceso implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de

comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.

Estructura del Proceso de Gestión de Riesgo

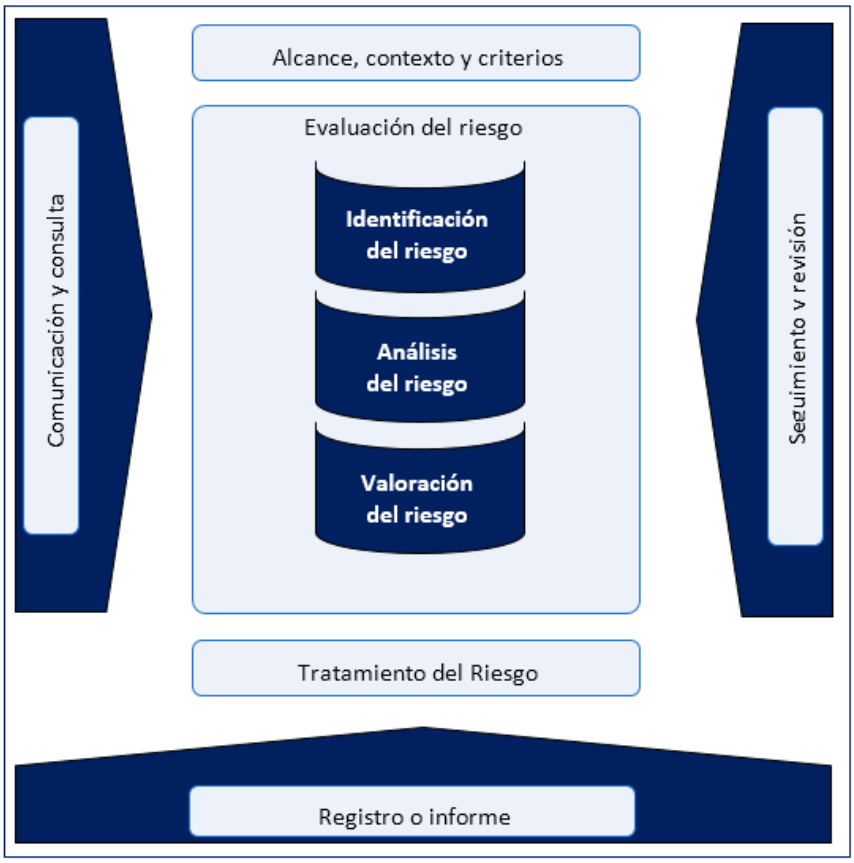

Figura No. 1 *La* Norma en referencia, estructura metódicamente el proceso de Gestión de Riesgos.

Definiciones de los elementos utilizados en la figura No. 1:

- **Alcance, contexto y criterios**: consiste en definir el alcance del proceso y comprender los contextos externo e interno.
- **Identificación del Riesgo**: tiene como propósito encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos.
- **Análisis del Riesgo**: Implica considerar en detalle la incertidumbre, fuentes de riesgo, consecuencias, probabilidad, eventos, escenarios, controles y su eficacia. Proporciona una entrada para la valoración del riesgo, para las decisiones sobre la manera de tratar los riesgos y los métodos más apropiados de tratamiento del riesgo. Los resultados proporcionan un entendimiento para la toma de decisiones. Las técnicas de análisis pueden ser cualitativas, cuantitativas o la combinación de ambas.

- **Valoración del Riesgo**: implica comparar los resultados del análisis con los criterios del riesgo para determinar la acción adicional.
- **Tratamiento del Riesgo**: puede implicar una o más de las acciones como evitar el riesgo, aceptar, eliminar compartir y retener el riesgo.

2. MARCO DE REFERENCIA MAGERIT

MAGERIT, está relacionada con la generalización del uso de las tecnologías de información, permitiendo conocer lo que está en juego en cuanto a los activos de información se refiere, por lo que ayudara a protegerlo y conocer el riesgo que están sometidos.
El marco de MAGERIT recomienda algunas técnicas para el análisis y gestión de riesgos, que para el presente proyecto se ha seleccionado utilizar el análisis mediante tablas, así como la realización de reuniones con personal del área de tecnología.
Además, define como elementos del riesgo los activos, amenazas, valor, degradación, impacto, probabilidad y con esos elementos define el riesgo del activo.
Otro aspecto del marco de MAGERIT y que es importante hacer notar es la dependencia de los activos que pone en la parte más alta los servicios que presta y que se refiere a todos los procesos y explica que en cada proceso existen datos y que hay datos que pueden relacionarse con dos procesos, que si existen amenazas en dichos datos la amenaza puede incidir en varios procesos, en el siguiente nivel se encuentran los equipos donde se almacenan los datos y las aplicaciones que hacen uso de los datos, como se ilustra en el siguiente graficó:

Modelo de dependencias Magerit

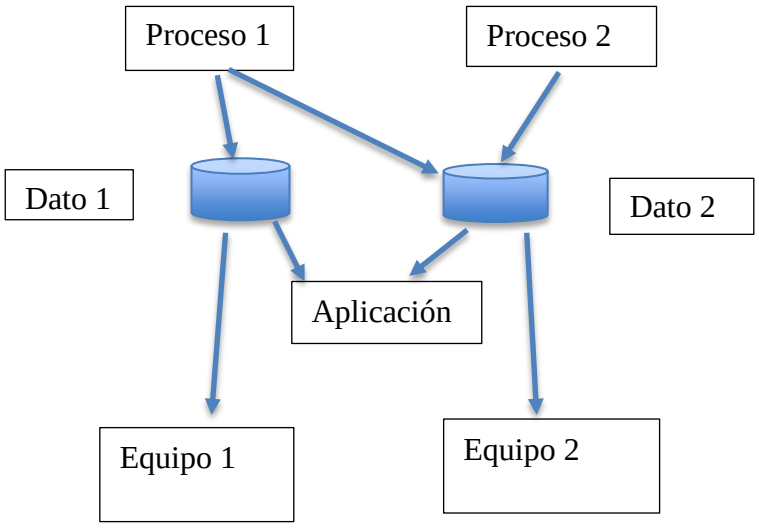

Figura No. 2 Modelo de dependencias Magerit

A continuación, se ilustra el proceso lógico del análisis de riesgo definido por el marco de MAGERIT, y define que no hay dos sistemas de información iguales, determina que el análisis de riesgo proporciona la visión de cómo es cada activo de información y el valor que posee, a qué amenazas está expuesto y los controles que se han aplicado.

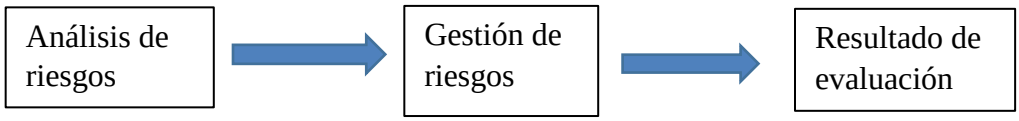

***Figura* No. 3** Proceso de gestión de riesgos

Análisis de riesgos, permite determinar qué tiene la Organización y estimar lo que podría pasar.

En la siguiente figura mostraremos los elementos que interviene en al análisis de riesgo

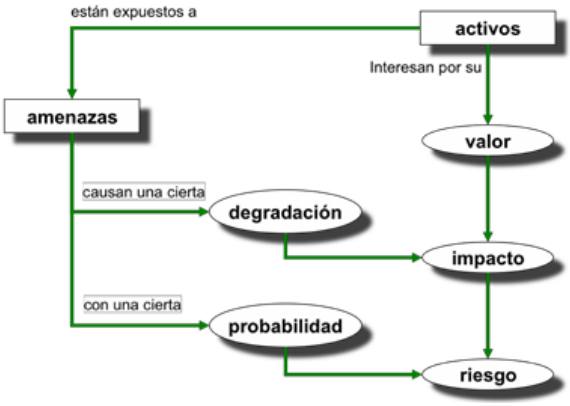

***Figura* No. 4** elementos del proceso de gestión de riesgos

tratamiento de los riesgos, permite organizar la defensa prudente, para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores

condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la alta Dirección asume.

Activos, son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización

Amenazas, cosas que les pueden pasar a los activos causando un perjuicio a la Organización

Salvaguardas o contramedidas, son medidas de protección para que las amenazas no causen tanto daño.

Impacto: consiste en lo que podría pasar

Riesgo: lo que probablemente pase

Después de realizar el análisis de riesgo en la que se determina el riesgo inherente y residual, se procede al estudio de los riesgos que lleva a la tomar acciones en el punto de decisión.

Esquema del Análisis de Riesgo

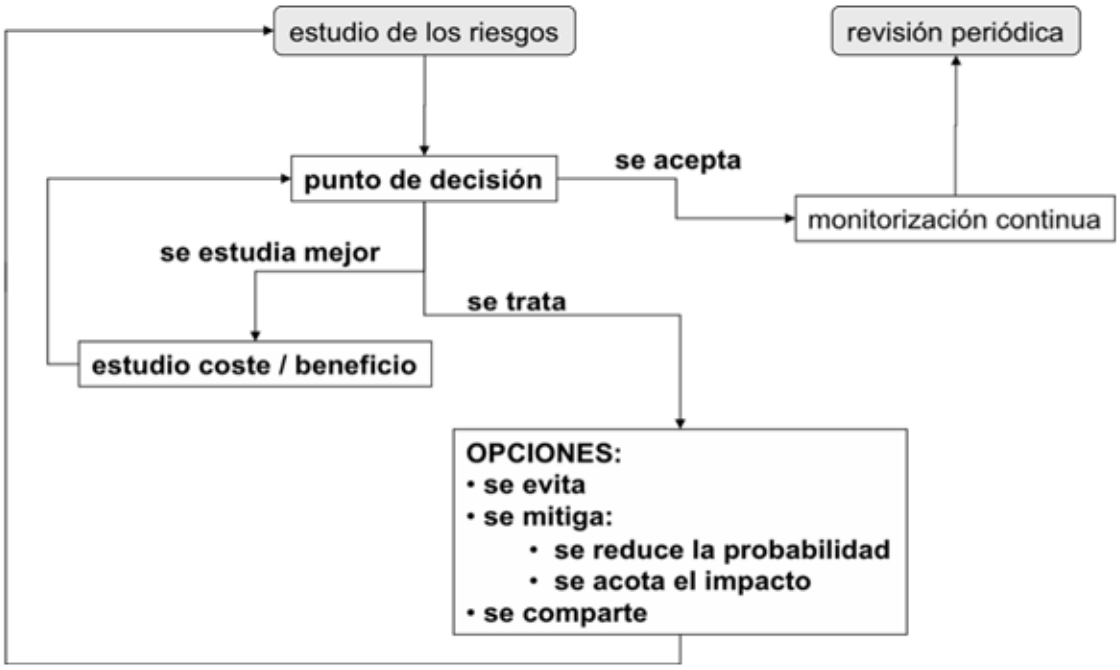

Figura No.5 Se ilustra el análisis de riesgo con el cual se determina el riesgo inherente y residual, para la tomar acciones en el punto de decisión

3. MARCO DE REFERENCIA COBIT 5

ISACA define el ciclo de vida de la gestión de riesgo de TI en cuatro pasos, que se muestran en la siguiente figura:

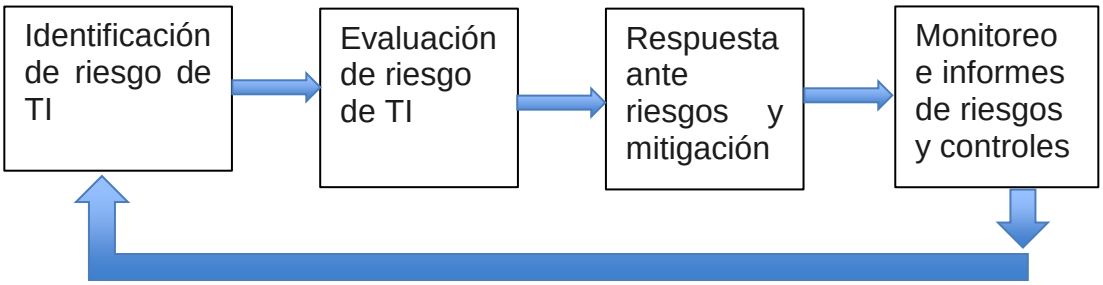

Figura 6. *Ciclo de vida de gestión del riesgo.*

El marco de referencia COBIT 5 nació 1996 con un enfoque de auditoría, para 1998 Cobit 2 agrega el control y Cobit 3 en el 2000 incluye la gestión y es del 2005 y 2007 que Cobit 4.0 y 4.1 incorpora el gobierno, en el 2009 se hace referencia al riesgo y al gobierno, para que con COBIT 5 en el 2012 se integran el gobierno, la gestión, el control y la auditoría.

COBIT 5 para riesgo, dentro del modelo de referencia de procesos en el dominio Evaluar, orientar y supervisar se identifica el proceso denominado "EDM03" Asegurar la Optimización del Riesgo; de igual forma en el dominio Alinear, Planificar y Organizar, se encuentra el proceso denominado "APO12" Gestionar el Riesgo, donde cada uno de dichos procesos cuenta con la descripción, la metas TI y sus métricas relacionadas, meta del proceso y métricas relacionadas, la matriz RACI para las prácticas de gobierno correspondientes, acompañadas de las actividades para alcanzar el propósito de cada proceso.
COBIT 5 clasifica los recursos de TI en aplicaciones, información, infraestructura y personas, los que intervienen en los procesos de TI, para el cumplimiento de las metas de TI.
El proceso "APO12" Gestionar el Riesgo, apoya la consecución de metas de TI y consiste en identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de los niveles de tolerancia establecidos por la alta dirección de la organización.
Dentro de las metas se encuentran:
APO12.01 Recopilar datos: identifica y recopila datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.

APO12.02 Analizar el riesgo: desarrollar información útil para soportar las decisiones relacionadas con el riesgo que toman en cuenta la relevancia para el negocio de los factores de riesgo.

CAPITULO IV. DESARROLLO DE LA METODOLOGIA

1. Estructura organizacional de la cámara de comercio e industria de el salvador.

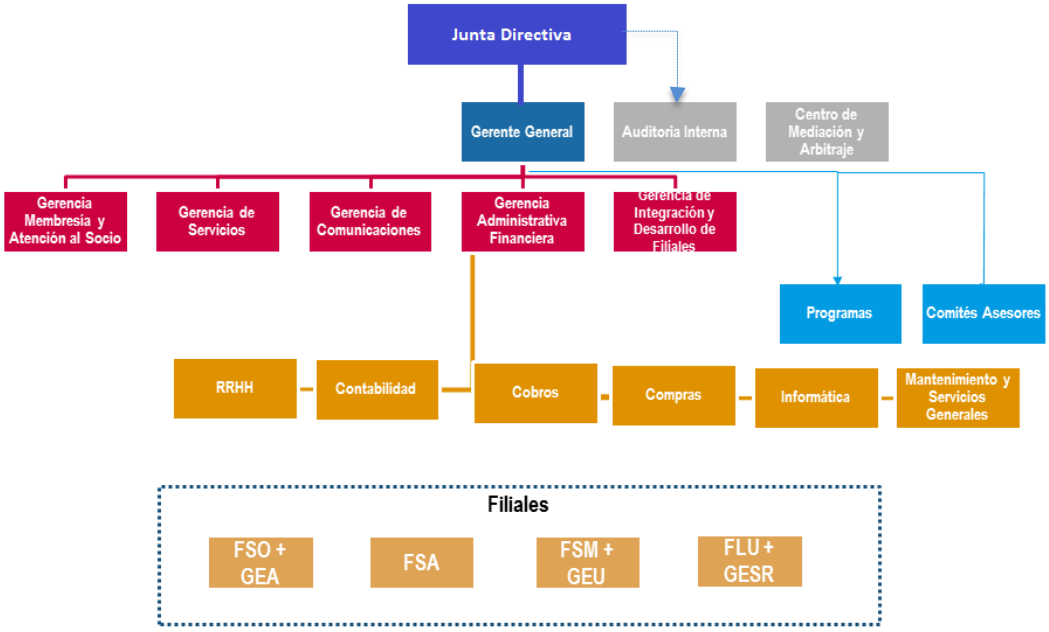

***Figura* No. 7** Organigrama de la CCIES

MISIÓN

Promover y defender permanentemente el sistema de libre iniciativa, impulsando la unidad nacional, y el desarrollo empresarial con responsabilidad social, liderando acciones y facilitando servicios que fomenten la competitividad y la innovación de nuestros asociados, protegiendo sus derechos.

VISIÓN

Ser la gremial líder y referente de la región, que contribuye a incrementar la competitividad de las empresas, fomenta el intercambio comercial y la inversión, generando las mejores oportunidades para su desarrollo con responsabilidad social.

2. Estructura organizacional propuesta para la gestión de riesgos en tecnología.

Para abordar los riesgos de la tecnología, no requiere que la alta Dirección sean expertos en TI, pero necesitan comprender sobre los riesgos, para vigilar y cuestionar sobre el control de estos.
Se recomienda, que debido a que no existe una unidad de Riesgos para gestionar los riesgos de tecnología sea la Gerencia General quien asigne a un responsable de la aplicación de la guía para gestionar los riesgos de tecnología, que no debe formar parte del Departamento de Informática y sea la Auditoria Interna quien lo audite.

Estructura funcional para la gestión de riesgo.

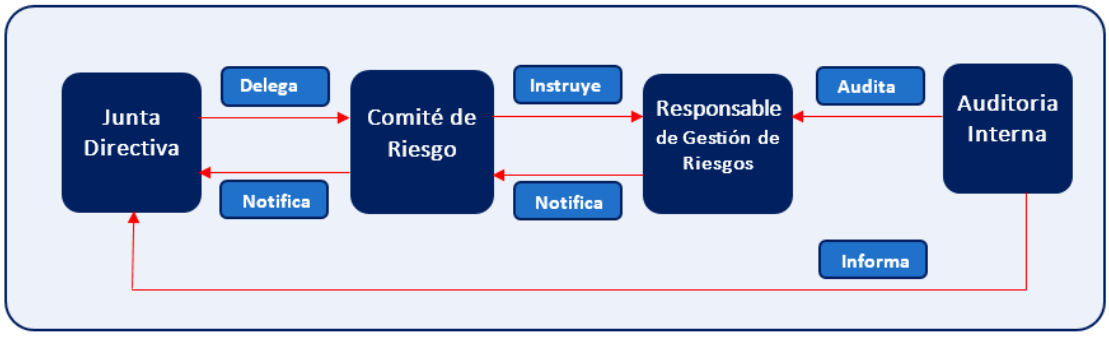

Figura 8. En la figura se muestra los entre los elementos que componen La Estructura funcional propuesta y sus relaciones (Roles).

3. Funciones de la estructura propuesta.

3.1. Funciones de la Junta Directiva

- Conocer todos los riesgos y su evolución y efectos sobre la tecnología de información, así como la metodología para gestionarlos.
- Aprobar la metodología para el análisis y gestión de riesgos de tecnología de la Información.
- Aprobar la estructura organizacional y funcional para la gestión de los Riesgos de Tecnología de la Información, asignando los recursos necesarios para implementar de forma adecuada la gestión de los riesgos de tecnología de la información, incluyendo programas de capacitación.

- Aprobar los límites de exposición del riesgo en cuestión.
- Aprobar la asignación a la Auditoría Interna que mediante un especialista de Informática efectúe auditorías de cumplimiento a la metodología para la gestión de riesgo de Tecnología de la Información y la periodicidad de las auditorías.

3.2. Funciones de Auditoría Interna.

- Efectuar auditorías de cumplimiento de la metodología y gestión del riesgo de tecnología de la información.
- Comunicar los hallazgos a la Junta Directiva y efectuar seguimientos.
- Evaluar en las unidades del negocio la aplicación de procesos de gestión de riesgos
- Asegurar que los riesgos están identificados y gestionados de forma apropiada
- Revisión independiente y objetiva de la aplicación de las políticas y métodos de gestión de riesgos por el Comité riesgo y las unidades respectivas.

3.3. Funciones del Comité de Riesgos

- Proponer a la Junta Directiva la aprobación la Política de Gestión de Riesgos.
- Proponer a la Junta Directiva la aprobación de la Metodología para el análisis y gestión de riesgos.
- Someter a la aprobación de la Junta Directiva los límites de exposición a los riesgos de tecnología.
- Comunicar a la Junta Directiva los resultados de la evaluación de los riesgos en la infraestructura tecnológica y las acciones tomadas.
- El Comité de Riesgo deberá celebrar sesiones de forma trimestral y documentar las reuniones mediante actas de Comité.

3.4. Funciones del Responsable de Gestionar el Riesgo de tecnología de la información.

- Identificar, medir, monitorear e informar respecto a los riesgos de tecnología de la información.
- Diseñar y proponer al Comité de Riesgo, políticas y procedimientos necesarios para gestionar los riesgos de la tecnología de la información.
- Informar de forma periódica sobre la evolución de los riesgos asumidos de tecnología de la información incluyendo cambios en los factores de riesgos.

- Dar seguimiento periódico a las acciones correctivas para la mejora en la gestión de los riesgos de tecnología de la información.
- Elaborar y proponer Planes de contingencia y continuidad del negocio.
- Promover la cultura de riesgo de tecnología

4. Política general de la gestión de riesgo de tecnología de la información.

4.1. Objetivo General:

- Definir lineamientos generales para la adecuada ejecución de la metodología de gestión de riesgos de tecnología de la información con el objeto de reducir la vulnerabilidad ante situaciones externas como internas relacionadas con la tecnología que puedan afectar el normal desempeño del servicio que presta la Cámara de Comercio e Industria de El Salvador.

4.2. Objetivos Específicos:

- Proteger los recursos de aplicaciones, información, infraestructura y personas, los que intervienen en los procesos de TI, para el cumplimiento de las metas de TI.
- Actuar de forma preventiva ante la posibilidad de ocurrencia de incidentes de riesgo de tecnología de la información.
- Establecer las directrices para el registro de incidentes relacionados con la tecnología de la información para ser utilizados en evaluaciones periódicas que permitan mejora de los servicios de tecnología.
- Establecer una cultura de prevención de los riesgos de la tecnología de información que está expuesta la organización.

4.3. Lineamientos de la Política:

- Se establece que la aplicación de la metodología contenida en el documento “Guía para la gestión de riesgos de tecnología” forma parte de las políticas para gestionar los riesgos de tecnología de la información.
- Se establece que todos los riesgos de tecnología de la información deben ser identificados, analizados, y establecer sus medidas de mitigación para reducir pérdidas derivadas de la materialización de algún incidente de riesgos relacionados con la tecnología de la información y deberá definir y aplicar controles para su monitoreo y comunicación.
- Los Gerentes y jefes son los responsables de registrar y comunicar al responsable de la Gestión de Riesgo de

Tecnología de la información, todos los incidentes relacionados con los recursos, aplicaciones, información, infraestructura y personas.

- Cuando el Departamento de Informática desarrolle nuevos procedimientos, aplicaciones y controles, o cambios en la infraestructura, deberá comunicarlo por escrito, al responsable de la gestión de riesgos de tecnología de la información, incluyendo los riesgos asociados.
- El encargado de la Gestión de Riesgo de Tecnología de la Información deberá presenta informes trimestrales a la Gerencia General con los resultados de la gestión.

5. Proceso para la evaluación de los riesgos de TI

5.1. Definición de la matriz de responsabilidades (RACI)

	DESCRIPCIÓN
Responsable (R)	Realiza el trabajo y sus tareas, debe existir solo una "R"
Autoriza/aprueba (A)	Se encarga de aprobar el trabajo finalizado, es quien debe asegurar que se ejecuten las tareas.
Consultado (C)	Posee información o la capacidad necesaria para terminar el trabajo, se le consulta información (comunicación bidireccional).
Informado (I)	Se le debe informar sobre el progreso de los resultados del trabajo, la comunicación es unidireccional.

Tabla 2. Definiciones de Responsabilidades en la Matriz RACI

TAREA	Junta Directiva	Jefe de Informática	Gerente General	Comité de Riesgo	Responsable de Gestionar el Riesgo	Personal de Informática
Aprobación de la estructura funcional para la gestión de riesgos	A		R			
Aprobación las funciones y responsabilidades de la estructura funcional	A		R			
Aprobar la Política General de la Gestión de Riesgo de Tecnología de la Información	A		R			
Recopilar datos de activos		C	I	A	I	R
Analizar el riesgo		C	I	A	R	I
Mantener un perfil de riesgo		C	I	A	R	I
Expresar el riesgo		C	I	A	R	I
Definir un portafolio de acciones para la gestión de riesgos		C	I	A	R	I
Responder al riesgo		C	I	A	R	I
Resultados de la evaluación de Riesgos	A	I	I	A	R	

Tabla 3. Matriz RACI (R: Responsable, A: Autoriza, C: consultado, I: Informado)

5.2. Identificar activos y determinar su valor

Para la recopilación de los datos del activo, se recomienda realizar entrevista a elementos de la Organización que se citan a continuación:

- **Dirección o Gerencia**, que conocen las consecuencias para la misión de la Organización
- **Responsable de los datos**, que conocen las consecuencias de sus fallos de seguridad.
- **Responsable de los servicios**, que conocen las consecuencias de la no prestación del servicio o de su prestación degradada.

- **Responsable de sistemas de información y responsables de operación**, que conocen las consecuencias de un incidente.

5.2.1. Clasificar Activos

Para la identificación de los activos, se deberá usar la siguiente clasificación:

- *Activos Primarios:*

En esta clasificación se agrupan todos los servicios y procesos de Tecnología.

- *Activos Secundarios:*

    - Datos que materializan la Información, agrupa los datos necesarios para la empresa como: registros de la empresa, datos personales, datos clasificados, datos críticos.
    - Equipo informático (Hardware).
    - Aplicaciones que permiten procesar los datos (Software).
    - Red de comunicación (permiten el intercambio de datos).
    - Soportes de información (dispositivos de almacenamiento de datos).
    - Instalaciones físicas que resguardan los equipos informáticos y de comunicación.
    - Personal que explota u opera todos los elementos anteriores.

5.2.2. Dimensiones de valoración

Las dimensiones son características o atributos que hacen valioso a un activo y se utilizan para estimar las consecuencias de la materialización de una amenaza; una vez clasificados los activos, el siguiente paso a realizar, es identificar las características de los activos.

- *Disponibilidad:* Propiedad o característica del activo (todo tipo de activo), que asegura que pueda estar disponible a personas, entidades o procesos autorizados. Se asigna el valor de “alto” al activo, sí una amenaza afectará a su disponibilidad y las consecuencias serían graves. Por el contrario, se asigna un valor de “bajo”, cuando puede no estar disponible frecuentemente y durante largos períodos de tiempo sin causar mayor.

- *Integridad:* Propiedad o característica del activo de información que consiste en que el activo no se ha alterado de manera no

autorizada. Por lo que se le asigna un valor “alto” cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización. Y se asigna un valor “bajo” cuando su alteración no causa preocupación alguna.

- *Confidencialidad*: Propiedad o característica que indica que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Se asigna un valor alto cuando su revelación causaría daños graves a la organización, por el contrario, se asigna un valor bajo cuando su revelación no afecta a la organización.

- *Autenticidad o no repudio:* garantiza la procedencia de la fuente de la información, en consecuencia, se asigna un valor alto cuando un defecto en el origen causaría graves daños a la organización, al contrario, se asigna un valor bajo, si el defecto en el origen no causa daños a la organización.

Nota: Para los activos clasificados como “servicio”, se debe tomar en consideración los criterios siguientes:

- Asignar un valor alto a un servicio, cuando se proporciona a usuarios no autorizados, causando un grave perjuicio para la organización.

- Se asigna un valor bajo cuando su acceso, por usuarios no autorizados no causa preocupación alguna.

CRITERIOS DE VALORACION DEL ACTIVO

Valor		Criterio
10	**EXTREMO**	**Daño extremadamente grave**
9	**MUY ALTO**	**Daño muy grave**
6-8	**ALTO**	**Daño grave**
4-5	**MEDIO**	**Daño importante**
2-3	**BAJO**	**Daño menor**
0-1	**DESPRECIABLE**	**Daño irrelevante a efectos prácticos**

Tabla 4. Valoración de dimensiones de los activos

5.2.3. Registrar las características dimensiones

Para cada activo se deberá registrar en la ficha de registro de activos del anexo I, con las siguientes características:

- Código, típicamente procedente del inventario

- Nombre (corto)
- Tipo (primario/secundario)
- Descripción (proceso, información, hardware software, red, personal e instalaciones físicas)
- Propiedad (Disponibilidad, Integridad, confidencialidad, autenticidad o no repudio)
- Valoración en función de la propiedad (alto o bajo)
- Unidad / Persona responsable
- Ubicación, técnica (en activos intangibles) o geográfica (en activos materiales)
- Cantidad (ejemplo 35 equipos)

Para registrar las valoraciones de las dimensiones (características) de los activos, se recomienda auxiliarse del catálogo, la tabla de dimensión y la ficha de registro de Activos, que se encuentran en el Anexo I.

5.3. Identificar las amenazas y valorarlas

Las amenazas son eventos o sucesos que pueden causar un daño o perjuicio a un activo. Para la gestión de riesgos es importante identificar, clasificar y valorar las amenazas a las cuales están expuestos los activos.

5.3.1. Identificar y clasificar las amenazas

- **De origen natural:** Hay accidentes naturales (terremotos, inundaciones, etc.). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

- **Del entorno (de origen industrial):** Hay desastres industriales (contaminación, fallos eléctricos, etc. ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- **Defectos de las aplicaciones** Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’

- **Causadas por las personas de forma accidental:** Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- **Causadas por las personas de forma deliberada:** Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

5.3.2. Valoración de las amenazas

Cuando una amenaza perjudica a un activo, no lo afecta en el mismo grado para todas sus dimensiones, ni en todas sus dimensiones.
Para valorar la influencia que una amenaza tiene sobre el valor de un activo, se debe considerar la degradación y la probabilidad descrito a continuación:

CRITERIOS DE VALORACION DE LA DEGRADACION

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción".

- **Degradación**: Consiste en estimar el grado de daño causado por la amenaza sobre el valor del activo.

Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo, para calcular la pérdida proporcional de valor que se pierde, pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna, pues el atacante puede causar muchísimo daño de forma selectiva. Por lo que se aplican los criterios a continuación:

Valor		Criterios	
MA	**MUY ALTO**	**Casi seguro**	**Fácil**
A	**ALTO**	**Muy alto**	**Medio**
M	**MEDIO**	**Posible**	**Difícil**
B	**BAJO**	**Poco probable**	**Muy difícil**
MB	**MUY BAJO**	**Muy raro**	**Extremadamente difícil**

Tabla 5. Valoración de la degradación de los activos

CRITERIOS DE VALORACION DE LA PROBABILIDAD

- **Probabilidad**: Estimar la frecuencia de ocurrencia de la materialización de la amenaza, sobre el activo.

La probabilidad de ocurrencia se suele de expresar o modelar cualitativamente por medio de una escala nominal, como se muestra en la tabla a continuación:

Valor			Criterios
MA	**Seguro**	**100**	**Muy frecuente (a diario)**
A	**Probable**	**10**	**Frecuentemente (semanalmente)**
M	**Posible**	**1**	**Normal (mensualmente)**
B	**Poco probable**	**1/10**	**Poco frecuente (una vez al año)**
MB	**Muy raro**	**1/100**	**Muy poco frecuente (cada varios años)**

Tabla 6. Valoración de probabilidad de ocurrencia.

5.3.3. Registrar las amenazas

Para cada amenaza se deberá registrar en una tabla, la siguiente información:

- Código
- Nombre de la amenaza
- La probabilidad de materialización de la amenaza
- El grado de degradación que causaría si se materializa
- Descripción del efecto de la amenaza

Para registrar las amenazas, se recomienda auxiliarse del catálogo y ficha de amenazas, que se encuentran en el Anexo II.

5.4. Identificar y Registrar el impacto potencial.

El grado del daño causado a un activo, al materializarse una amenaza se denomina **impacto.**

El impacto de las amenazas sobre los activos se puede determinar conociendo el valor de los activos (en sus dimensiones) y la degradación que causan las amenazas.

Se debe tomar en consideración la dependencia de los activos entre sí, ya que las amenazas suelen materializarse en los medios (relación de dependencia entre activos)

El siguiente paso corresponderá en Identificar, la medida en que un activo clasificado como primario puede ser perjudicado por una amenaza materializada sobre un activo clasificado como secundario. La medida propuesta es alto (100%), medio (10%), Baja (1%), la que deberá documentar los factores del valor asignado.

5.4.1. Estimar el impacto potencial

Estimar el impacto definido como el daño sobre el activo derivado de la materialización de la amenaza.

En este paso se deberá estimar el impacto de acuerdo con la siguiente tabla:

IMPACTO		DEGRADACION		
		1%	10%	100%
VALOR	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 7. Estimación del impacto potencial

Para cada activo se deberá registrar en una tabla, el impacto potencial, con la siguiente información:

- Código del activo
- Nombre del activo
- Matriz de impacto

Para registrar el impacto potencial por activo, se recomienda auxiliarse de la tabla estimación del impacto, que se encuentran en el Anexo III.

5.5. Identificar y Registrar el riesgo potencial.

5.5.1. Estimar el riesgo potencial

En esta actividad se estiman los siguientes riesgos:

- El riesgo potencial, al que está sometido el activo teniendo en cuenta su valor y el valor de las amenazas; pero no los controles.
- El riesgo residual, al que está sometido el activo tomando en cuenta su valor y el valor de las amenazas, así como la eficacia de los controles.

Para la estimación del riesgo se recomienda utilizar la escala a continuación:

ESCALAS		
Impacto	**Probabilidad**	**Riesgo**
MA: Muy alto	MA: Seguro	MA: Crítico
A: Alto	A: Probable	A: Grave
M: Medio	M: Posible	M: Apreciable
B: Bajo	B: Poco probable	B: Bajo
MB: Muy bajo	MB: Muy raro	MB: Despreciable

Tabla 8. Escala para estimación del riesgo.

En la combinación de las valoraciones del impacto y de probabilidad se determina el riesgo con la siguiente tabla:

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 9. Estimación del riesgo potencial.

- Cuando se obtiene el riesgo como crítico (MA), requiere atención urgente.
- En el caso que el resultado sea grave (A), se deberá monitorear.
- En el caso que sea apreciable se deberán estudiar más opciones.
- Y si es asumible en el sentido que no se tomarán acciones para reducir el impacto.

Para cada activo se deberá registrar en una tabla, el riesgo potencial, con la siguiente información:

- Código del activo
- Nombre del activo
- Matriz de riesgo

Para registrar el riesgo potencial por activo, se recomienda auxiliarse de la tabla estimación del riesgo, que se encuentran en el Anexo III.

5.6. Salvaguardas.

Se definen las salvaguardas o contra medidas a los procedimientos o mecanismos tecnológicos que reducen el riesgo.

5.6.1. Determinar los controles y su eficiencia frente a cada amenaza de riesgo.

Para cada control se debe documentar la siguiente información:

- Código
- Nombre
- Tipo de Control, describe el efecto del control
- Estado de implantación
- Eficiencia
- La amenaza
- Descripción del control

Se deberá registrar cada control, en la Ficha de Controles, para realizar esta actividad se recomienda auxiliarse del Catálogo de Controles, la Tabla de Tipos de Controles y la Tabla de eficiencia y madurez de los controles que se encuentran en el Anexo IV.

CRITERIOS DE EVALUACIÓN DE LOS CONTROLES

El proceso para establecer el porcentaje de cumplimiento de cada uno de los controles presentes en la lista de controles se tendrá en cuenta los niveles de madurez de procesos establecidos en la norma ISO/IEC 27001:2013 Anexo A, y para realizar la evaluación se utilizarán los criterios que se muestra a continuación:

Porcentaje	Criterio	Descripción
0%	No realizado	No hay controles de seguridad de la información establecidos.
20%	Realizado informalmente	Existen procedimientos para llevar a cabo ciertas acciones en determinado momento. Estas prácticas no se adoptaron formalmente y/o no se les hizo seguimiento y/o no se informaron adecuadamente.
40%	Planificado	Los controles de seguridad de la información establecidos son planificados, implementados y repetibles.
60%	Bien definido	Los controles de seguridad de la información además de planificados son documentados, aprobados e implementados en toda la organización.
80%	Cuantitativamente controlado	Los controles de seguridad de la información están sujetos a verificación para establecer su nivel de efectividad.
100%	Mejora continua	Los controles de seguridad de la información definidos son periódicamente revisados y actualizados. Estos reflejan una mejora al momento de evaluar el impacto.

Tabla 10. Criterios de Evaluación de los controles

En el Anexo IV se detalla cada uno de los controles, aplicando los criterios de la tabla de criterios de evaluación.

Posterior a la evaluación de los controles recomendados en la ISO/IEC 27001:2013 se obtendría un gráfico que estaría mostrando el estado de madurez de los controles aplicados.

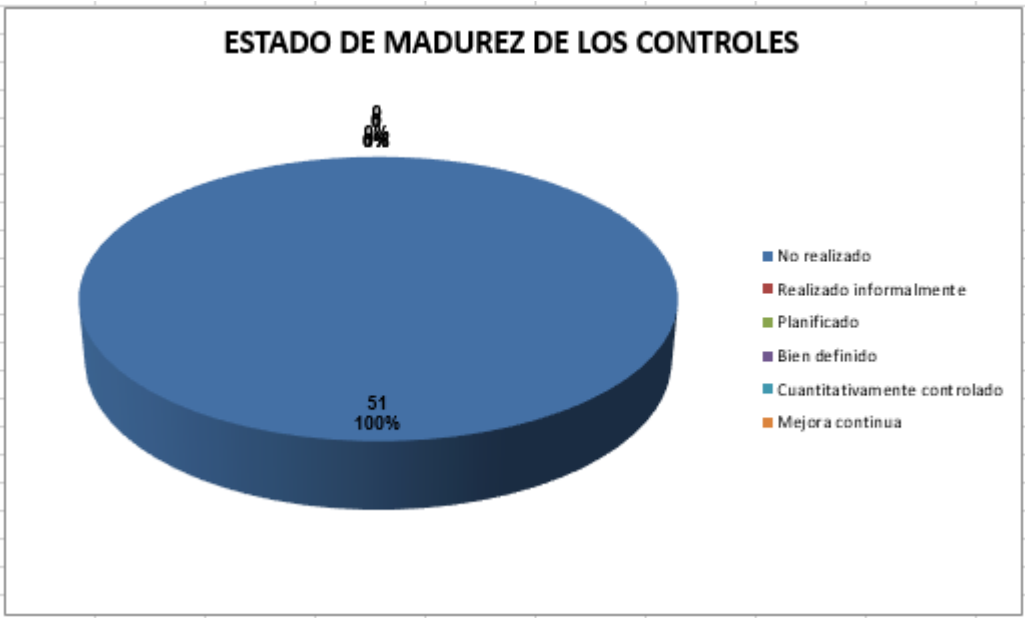

Figura 9. En la figura se muestra el resultado de la madurez de los controles aplicados.

5.7. Impacto Residual.

Con la aplicación de un conjunto de controles y la madurez del proceso de gestión de riesgos, el sistema queda en una situación de impacto que se denomina residual, se dice que es la modificación del impacto potencial a un impacto residual.

Cálculo del impacto residual
Como ya se determinaron los activos, solamente cambia la magnitud de la degradación, y se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

5.8. Riesgo Residual.

Con la aplicación de un conjunto de controles y la madurez del proceso de gestión de riesgos, el sistema queda en una situación de riesgo que se denomina residual, se dice que es la modificación del riesgo potencial a un riesgo residual.

Cálculo del riesgo residual

Como ya se determinaron los activos, solamente cambia la magnitud de la degradación y la posibilidad de materialización de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación tomando en cuenta el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

5.9. Determinar las acciones a realizar de acuerdo con los resultados de la estimación.

En consecuencia, a la gravedad del impacto y los riesgos, se deberá proceder con el tratamiento de los riesgos y tomar una serie de acciones condicionadas a diversos factores:

a) Aceptar ciertos impactos de naturaleza intangible tales como:

- Imagen pública de cara a la Sociedad (aspectos de reputaciones)

- Política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.

- relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.

- Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia.

- relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.

La aceptación del riesgo siempre es arriesgada y hay que tomarlo con prudencia y justificación. Se recomienda considerar reservar fondos para el caso que el riesgo se concrete y haya que responder ante sus consecuencias. Las razones para su aceptación son:

- Cuando el impacto residual es asumible
- Cuando el riesgo residual es asumible.
- Cuando el costo del control oportuno es desproporcionado en comparación al impacto y el riesgo residual.

b) En el caso de decidir transferir el riesgo:

- Se comparte por medio de la contratación de seguros, de forma que, a cambio de una prima, se reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Según el acuerdo que se establezca.

c) Si se decide mitigar el riesgo se debe cumplir una de dos opciones:

- Reducir el impacto causado por una amenaza.
- Reducir la probabilidad que una amenaza se materialice.

d) Otro tratamiento del riesgo consiste en la eliminación de la fuente de riesgo, opción frente a un riesgo que no es aceptable. Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos y utilizar otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos, etc.
- Reordenar la arquitectura del sistema (el esquema de dependencias) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, separar equipos para atender necesidades concretas, en general alejando el activo más valioso de lo más expuesto.
- La eliminación de las fuentes de riesgo, obliga a realizar un nuevo análisis de riesgos sobre el sistema modificado.

5.10. Comunicar el resultado.

Los resultados deberán comunicarse mediante un informe ejecutivo, de la gestión de riesgos en sobre los procesos de tecnología, se recomienda expresarlos de forma gráfica, destacando los de mayor impacto, los riesgos asumidos, los tipos de activos afectados, sus amenazas y los controles aplicados.

5.11. Oportunidad de Mejora Continua

Durante todo el desarrollo de la presente metodología de riesgos de tecnología, se cumple el denominado Ciclo de Deming.

Ciclo de Deming

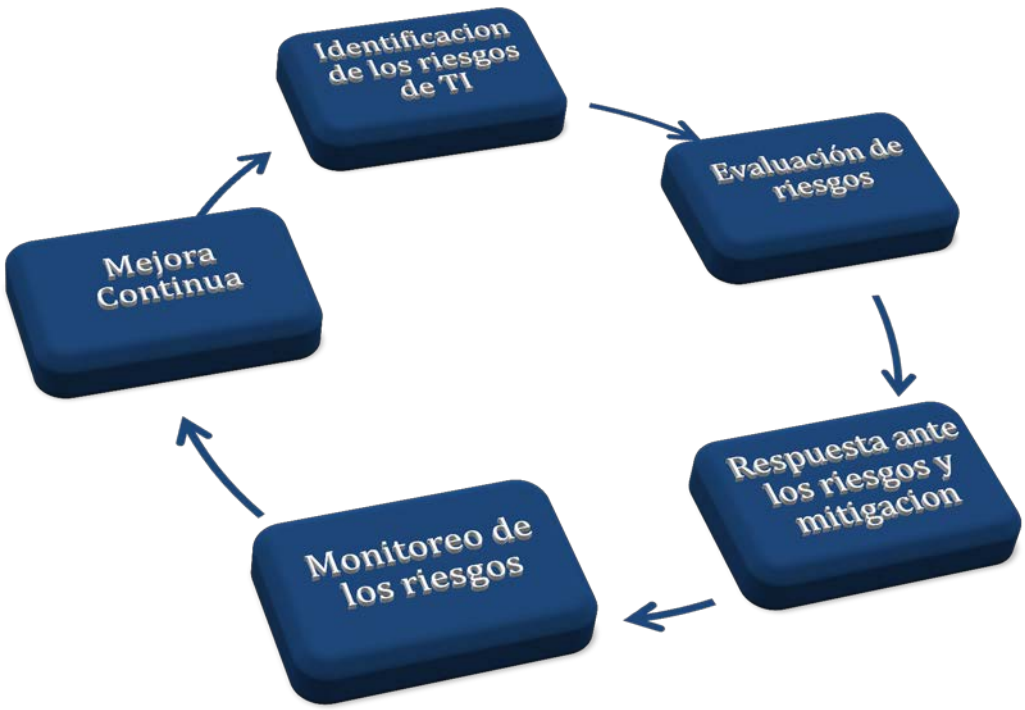

Figura 10. Muestra el Ciclo de Deming, que representa la metodología del riesgo.

Con la evolución de las tecnologías y los servicios, pueden surgir nuevas amenazas o convertir amenazas no relevantes en relevantes en el futuro, lo que requerirá evaluar las condiciones de explotación de las amenazas.
Por lo anterior, la Organización, deberá continuamente efectuar seguimientos para la mejora de la idoneidad, adecuación y efectividad de la metodología aplicada al gestionar los riesgos que podrían vulnerar la seguridad de la información por deficiencias en la infraestructura tecnológica, se deberá aplicar evaluaciones del grado de madurez de los controles aplicados, tomando en cuenta los que se encuentran en la tabla detallada en el numeral 3. Catálogo de controles, para ello se hará uso de tabla en Excel que se anexa, tomada de la ISO/IEC 270001:2013 Anexo A.
Una vez obtenido el resultado de la evaluación de los controles como se muestra en el numeral 4 Evaluación de aplicación de controles, se deberá nuevamente realizar la evaluación de los riesgos y determinar las acciones a realizar en función de los nuevos resultados obtenidos.

5.12. Apetito de Riesgo

La CCIES, no ha implementado un sistema de gestión integral de riesgos, sin embargo, ha mostrado interés por la propuesta de una guía basada en metodologías de gestión de riesgos tecnológicos, es por ello por lo que previo a la aplicación de la guía de evaluación de riesgos de tecnología.

La alta Gerencia y la Junta Directiva deberán determinar el umbral de aceptación del apetito de riesgo de la organización, con los que la CCIES procederá a gestionar el riesgo de tecnología.

Bajo ese contexto, se deberá someter a consideración la siguiente propuesta para la CCIES del apetito de riesgo:

- Los riesgos con incidencia bajo se aceptan, cuando se estima que la probabilidad de que ese riesgo se materialice en probable y seguro;

- Los riesgos con incidencia medio se aceptan cuando se estima que la probabilidad de que ese riesgo se materialice es poco probable y posible;

- Los riesgos con incidencia alto se aceptan únicamente cuando se estima que la probabilidad de que ese riesgo se materialice es muy rara.

Los riesgos antes referidos, solo se deberán aceptar mediante la respectiva aprobación, cuando se cercioren de que las medidas de mitigación aplicadas son las adecuadas.

Además, del umbral de aceptación del riesgo, se deberá incluir en la solicitud de aprobación las acciones a realizar cuando resulte el riesgo como Critico, el cual requerirá atención urgente y en el caso que se obtenga como grave, se deberá monitorear, de igual forma agregar las siguientes consideraciones:

Todo riesgo que vaya más allá del apetito de riesgo de la CCIES será evaluado por los Gerentes y/o el Comité de Riesgos de la CCIES, tomando en cuenta la tolerancia al riesgo.

Para mantener la prestación de servicios con los afiliados y ampliar el número de usuarios, es de importancia fundamental que esos servicios sean de elevada calidad, seguros y económicos. La CCIES está comprometida en proteger los datos que se le confían, y tiene tolerancia cero respecto de cualquier riesgo identificable que pueda poner en peligro la confidencialidad o la integridad de los datos.

CAPITULO V RESULTADOS

Caso de uso: Proceso de Respaldo de Información.

El proceso para la realización de respaldos en la Cámara de Comercio e Industria de El Salvador es manual no existe proceso sistematizado por tal motivo dicho proceso se realiza una vez al año lo cual se programa a mediados del año.
Se crea un cronograma con las fechas posibles en las que se estaría visitando en cada estación de trabajo dividido por departamentos para no frenar las operaciones del departamento, este cronograma es presentado y aprobado por la Gerencia General y con visto bueno se procede a realizar la divulgación a cada Gerente para que se dé por enterado las fechas a realizar el respaldo a cada uno de los miembros de su departamento, si hubiese la necesidad de cambiar alguna fecha por que la persona no estará y es laptop el equipo, se cambia de fecha con alguna otra persona del mismo departamento. Una vez el cronograma ha sido modificado se reenvía al área o departamento en donde hubo modificaciones para que se dé nuevamente el visto bueno.
Luego se procede a realizar el respaldo, como se realiza: el personal de IT se traslada al lugar de la estación a la que se le realizara el respaldo y previa selección de la información a respaldar por parte del usuario, se crea en el disco duro externo una carpeta con el nombre del usuario y se traslada la información seleccionada por el usuario, una vez finalizado el proceso el usuario firma de que se realizó el respaldo como comprobante del personal de IT y se procede a continuar con el siguiente usuario al que se le ha asignado en el cronograma. Una vez finalizado el proceso en todos los departamentos se procede a guardar en un lugar seguro y libre de humedad el disco externo.

***Figura* No. 10** elementos del proceso de gestión de riesgos, en el proceso de respaldo de información de usuario

IDENTIFICACIÓN Y VALORACION DE ACTIVOS

[S] Servicio	
Código: 00001	**Nombre:** Proceso de Respaldo de datos e información
Tipo: Activo Primario	
Descripción: El Procedimiento de respaldo de información de usuario, tiene por objetivo salvaguardar la información que el usuario estima como importante y valiosa. La información de los usuarios es ubicada en un solo repositorio (disco duro extraíble), debido a lo anterior la información de usuarios claves, está expuesta. Para el proceso se establece una programación anual. El encargado de realizar el respaldo se desplaza al equipo del usuario, y copia la información a un disco duro extraíble. El proceso podría fallar si el encargado de realizar el proceso no tiene claro el proceso o no se encuentra disponible para efectuarlo, también puede que falle si el dispositivo de almacenamiento no funciona adecuadamente o si el equipo del usuario no se encuentra accesible.	
Propiedad: Son las características o atributos que hacen valioso el activo, estas son Disponibilidad, Confidencialidad, Autenticación.	
Valoración: Disponibilidad: Extremo (10) Confidencialidad: Extremo (10) Autenticación: Medio (5) daño importante	
Unidad / Persona Responsable: Soporte de Informática	
Ubicación: Departamento de TI	
Cantidad: 1 copia	

Tabla 11. Identificación y valoración de Activo 1

[P] Personal

Código: 00002	**Nombre:** Personal que realiza el respaldo
Tipo: Activo Secundario	
Descripción: Personal del área de soporte a cargo de realizar el proceso copias de respaldo	
Propiedad: Son las características o atributos que hacen valioso el activo, estas son: Confidencialidad y Autenticación.	
Valoración: Confidencialidad: Extremo (10) Autenticación: Medio (5)	
Unidad / Persona Responsable: Soporte de informática	
Ubicación: Departamento de informática	
Cantidad: 1 persona	

Tabla 12. Identificación y valoración de Activo 2

[Media] Soporte de información	
Código: 00003	**Nombre:** disco duro externo y aplicación para realizar el respaldo
Tipo: Activo Secundarios	
Descripción: Disco duro externo que almacena el respaldo de la información y la aplicación con la que se realiza el proceso de copiado de los datos e información.	
Propiedad: Son las características o atributos que hacen valioso ambos activos, estas son para la unidad de disco duro: Disponibilidad. Y para la aplicación que realiza la copia de respaldo: Disponibilidad y Autenticación	
Valoración: • **unidad de disco duro**: Disponibilidad: medio (5) daño importante • **aplicación que realiza la copia de respaldo**: Disponibilidad: Extremo (10) daño extremadamente grave	
Unidad / Persona Responsable: Soporte de Informática	
Ubicación: Departamento de Informática	
Cantidad: 1 disco duro y una licencia de la aplicación	

Tabla 13. Identificación y valoración de Activo 3

[D] Datos

Código: 00004	**Nombre:** Datos a respaldar
Tipo: Activo Secundario	
Descripción: Todos los datos e información de la CCIES que se respalda incluyendo contabilidad, sistemas/aplicaciones, transacciones con afiliados.	
Propiedad: Características o atributos que hacen valioso el activo datos a respaldar, estas son Disponibilidad, Integridad, Confidencialidad y Autenticación.	
Valoración Disponibilidad: Extremo (10) daño extremadamente grave Integridad: Extremo (10) daño extremadamente grave Confidencialidad: Extremo (10) daño extremadamente grave Autenticación: Extremo (10) daño extremadamente grave	
Unidad / Persona Responsable: Soporte de Informática	
Ubicación: Centro de datos	
Cantidad:	

Tabla 14. Identificación y valoración de Activo 4

IDENTIFICACCION, VALORACIÓN DE LAS AMENAZAS Y RIESGO POTENCIAL

[E] amenaza: Errores y fallos no intencionados	
Tipo de activo: [S] Servicio **Código activo:** 00001 **Nombre del activo:** Proceso de Respaldo de datos e información	Dimensiones de los activos que se ven afectadas por este tipo de amenaza a continuación: • Disponibilidad: Extremo (10) • Confidencialidad: Extremo (10) • Autenticación: Medio (5) daño importante
Detalle de Amenazas que se incluyen en la amenaza principal [E] Errores y fallos no intencionados: [E.2] Errores del administrador [E.4] Errores de configuración del proceso de copias de respaldo [E.7] Destrucción de información [E.8] Fugas de información [E.11] Caída del sistema por agotamiento de recursos, [E.12] Indisponibilidad del personal.	
Degradación: El grado de degradación que causaría si se materializan las amenazas [E.2] Errores del administrador: Poco probable **(B) Bajo** [E.4] Errores de configuración del proceso de copias de respaldo: Posible **(M) Medio** [E.7] Destrucción de información respaldada: Muy raro **(MB) muy bajo** [E.8] Fugas de información: Poco probable **(B) Bajo** [E.11] Caída del sistema por agotamiento de recursos: Muy Alto **(A) Alto** [E.12] Indisponibilidad del personal: Poco probable **(B) Bajo**	
Probabilidad: La probabilidad de ocurrencia de la amenaza [E.2] Errores del administrador: Poco probable **(B)** [E.4] Errores de configuración del proceso de copias de respaldo: Poco probable **(B)** [E.7] Destrucción de información respaldada: Muy raro **(MB)** [E.8] Fugas de información: Muy raro **(MB)** [E.11] Caída del sistema por agotamiento de recursos: Poco probable **(B)** [E.12] Indisponibilidad del personal: Posible (**M)**	
Descripción: el proceso de respaldo se puede ver afectado por las amenazas no intencionadas descritas, que afecten el desarrollo del proceso de generación de las copias de respaldo de la información, y a las copias mismas.	

Impacto Potencial:
para la amenaza de errores y fallos no intencionados es Muy bajo (MB)

[00001] Proceso de respaldo de datos e información						
IMPACTO		**DEGRADACIÓN**				
		1/100% (MB)	**1/10% (B)**	**1% (M)**	**10% (A)**	**100% (MA)**
VALOR DEL ACTIVO	**MA**	MB	B	M	A	MA
	A	MB	MB	B	M	A
	M	MB	MB	MB	B	M
	B	MB	MB	MB	MB	B
	MB	MB	MB	MB	MB	MB

MATRIZ DEL IMPACTO POTENCIAL DEL ACTIVO

<u>Riesgo Potencial</u> para la amenaza de Errores y fallos no intencionados es despreciable (MB)

[E.2] Errores del administrador, con probabilidad **(B)** e impacto **(MB)** el riesgo MB
[E.4] Errores de configuración del proceso de copias de respaldo, con probabilidad **(B)** e impacto el riesgo MB
[E.7] Destrucción de información, con probabilidad **(MB)** e impacto **(MB)** el riesgo MB
[E.8] Fugas de información, con probabilidad **(MB) e** impacto **(MB)** el riesgo MB
[E.11] Caída del sistema por agotamiento de recursos, con probabilidad **(B**) e impacto MB el riesgo MB
[E.12] Indisponibilidad del personal, con probabilidad (**M**) e impacto **(MB)** el riesgo MB

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Estimación del riesgo potencial

Tabla 15. Identificación y valoración de Amenaza 1

[N] amenaza: Desastres Naturales (inundación, incendio, terremotos)

Tipo: [Media] Soporte de información **Código activo:** 00003 **Nombre activo:** disco duro externo y aplicación para realizar el respaldo	Dimensiones de los activos que se ven afectadas por este tipo de amenaza a continuación: • **unidad de disco duro externo**: Disponibilidad: medio (5) daño importante • **aplicación que realiza la copia de respaldo**: Disponibilidad: Extremo (10) daño extremadamente grave
Degradación: El grado de degradación que causaría si se materializa la amenaza es Muy alta (MA)	
Probabilidad: La probabilidad de ocurrencia de la amenaza es seguro (MA)	
Descripción: que se pierda la información que se encuentra en los discos duros externos y se dañe de forma permanente la aplicación que realiza el respaldo.	
Impacto potencial: Muy Alto (MA)	
Riesgo potencial: para un impacto (MA) muy alto y una probabilidad (MA) Seguro se determina un riesgo potencial **de Critico (MA)**	

Tabla 16. Identificación y valoración de Amenaza 2

[A] amenaza: Ataques intencionados	
Tipo de activo: [S] Servicio **Código activo:** 00001 **Nombre del activo:** Proceso de Respaldo de datos e información	Dimensiones de los activos que se ven afectadas por este tipo de amenaza a continuación: • Disponibilidad: Extremo (10) • Confidencialidad: Extremo (10) • Autenticación: Medio (5) daño importante
Detalle de Amenazas que se incluyen en la amenaza principal [E] Errores y fallos no intencionados: [E.2] Errores del administrador [E.4] Errores de configuración del proceso de copias de respaldo [E.7] Destrucción de información [E.8] Fugas de información [E.11] Caída del sistema por agotamiento de recursos, [E.12] Indisponibilidad del personal.	
Degradación: El grado de degradación que causaría si se materializan las amenazas [E.2] Errores del administrador: Poco probable **(B) Bajo** [E.4] Errores de configuración del proceso de copias de respaldo: Posible **(M) Medio** [E.7] Destrucción de información respaldada: Muy raro **(MB) muy bajo** [E.8] Fugas de información: Poco probable **(B) Bajo** [E.11] Caída del sistema por agotamiento de recursos: Muy Alto **(A) Alto** [E.12] Indisponibilidad del personal: Poco probable **(B) Bajo**	
Probabilidad: La probabilidad de ocurrencia de la amenaza [E.2] Errores del administrador: Poco probable **(B)** [E.4] Errores de configuración del proceso de copias de respaldo: Poco probable **(B)** [E.7] Destrucción de información respaldada: Muy raro **(MB)** [E.8] Fugas de información: Muy raro **(MB)** [E.11] Caída del sistema por agotamiento de recursos: Poco probable **(B)** [E.12] Indisponibilidad del personal: Posible (**M)**	
Descripción: el proceso de respaldo se puede ver afectado por las amenazas no intencionadas descritas, que afecten el desarrollo del proceso de generación de las copias de respaldo de la información, y a las copias mismas.	
Impacto Potencial:	

para la amenaza de errores y fallos no intencionados es Muy bajo (MB)

[00001] Proceso de respaldo de datos e información						
IMPACTO		**DEGRADACION**				
		1/100% (MB)	**1/10% (B)**	**1% (M)**	**10% (A)**	**100% (MA)**
VALOR DEL ACTIVO	**MA**	MB	B	M	A	MA
	A	MB	MB	B	M	A
	M	MB	MB	MB	B	M
	B	MB	MB	MB	MB	B
	MB	MB	MB	MB	MB	MB

MATRIZ DEL IMPACTO POTENCIAL DEL ACTIVO

<u>Riesgo Potencial</u> para la amenaza de Errores y fallos no intencionados es despreciable (MB)

[E.2] Errores del administrador, con probabilidad **(B)** e impacto **(MB)** el riesgo MB
[E.4] Errores de configuración del proceso de copias de respaldo, con probabilidad **(B)** e impacto el riesgo MB
[E.7] Destrucción de información, con probabilidad **(MB)** e impacto **(MB)** el riesgo MB
[E.8] Fugas de información, con probabilidad **(MB) e** impacto **(MB)** el riesgo MB
[E.11] Caída del sistema por agotamiento de recursos, con probabilidad **(B**) e impacto MB el riesgo MB
[E.12] Indisponibilidad del personal, con probabilidad (**M**) e impacto **(MB)** el riesgo MB

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Estimación del riesgo potencial

Tabla 17. Identificación y valoración de Amenaza 3

RIESGO RESIDUAL

[S] Servicio	
Código: 00001	**Nombre:** Proceso de Respaldo de datos e información
Tipo: Activo Primario	
Descripción: El Procedimiento de respaldo de información de usuario, tiene por objetivo salvaguardar la información que el usuario estima como importante y valiosa. La información de los usuarios es ubicada en un solo repositorio (disco duro extraíble), debido a lo anterior la información de usuarios claves, está expuesta. Para el proceso se establece una programación anual. El encargado de realizar el respaldo se desplaza al equipo del usuario, y copia la información a un disco duro extraíble. El proceso podría fallar si el encargado de realizar el proceso no tiene claro el proceso o no se encuentra disponible para efectuarlo, también puede que falle si el dispositivo de almacenamiento no funciona adecuadamente o si el equipo del usuario no se encuentra accesible.	
Propiedad: Son las características o atributos que hacen valioso el activo, estas son Disponibilidad, Confidencialidad, Autenticación.	
Valoración: Disponibilidad: Extremo (10) Confidencialidad: Extremo (10) Autenticación: Medio (5) daño importante	
Unidad / Persona Responsable: Soporte de Informática	
Ubicación: Departamento de Informática	
Cantidad: 1 copia	

DEGRADACIÓN RESIDUAL

Salvaguardas:

[S] proteger el servicio de copias de respaldo, en cuanto a que esta disponibilidad (M) posible.
[S.A] Asegurar la disponibilidad de la aplicación para realizar las copias de respaldo, unidad de almacenamiento (disco duro externo), personal que ejecuta el proceso y la información a respaldar. (M) posible
[SS] Aceptación y puesta en operación del proceso de respaldo, autenticación y confidencialidad (M) posible

Valor		Criterios degradación Residual	
MA	MUY ALTO	Casi seguro	Fácil
A	ALTO	Muy alto	Medio
M	MEDIO	Posible	Difícil
B	BAJO	Poco probable	Muy difícil
MB	MUY BAJO	Muy raro	Extremadamente difícil

PROBABILIDAD RESIDUAL

[S] proteger el servicio de copias de respaldo, en cuanto a que esta disponibilidad (M) posible.
[S.A] Asegurar la disponibilidad de la aplicación para realizar las copias de respaldo, unidad de almacenamiento (disco duro externo), personal que ejecuta el proceso y la

información a respaldar. (M) posible
[SS] Aceptación y puesta en operación del proceso de respaldo, autenticación y confidencialidad (M) posible

Valor		Criterios de probabilidad Residual
MA Seguro	100	Muy frecuente (a diario)
A Probable	10	Frecuentemente (semanalmente)
M Posible	1	Normal (mensualmente)
B Poco probable	1/10	Poco frecuente (una vez al año)
MB Muy raro	1/100	Muy poco frecuente (cada varios años)

IMPACTO RESIDUAL

Valoración:
Disponibilidad: Extremo (10)
Confidencialidad: Extremo (10)
Autenticación: Medio (5) daño importante

Degradación:
[S] proteger el servicio de copias de respaldo, en cuanto a que esta disponibilidad (M) posible.
[S.A] Asegurar la disponibilidad de la aplicación para realizar las copias de respaldo, unidad de almacenamiento (disco duro externo), personal que ejecuta el proceso y la información a respaldar. (M) posible
[SS] Aceptación y puesta en operación del proceso de respaldo, autenticación y confidencialidad (M) posible

[S] SERVICIO						
IMPACTO		DEGRADACION				
		1/100% (MB)	1/10% (B)	1% (M)	10% (A)	100% (MA)
VALOR DEL ACTIVO	EX	MB	B	M	A	MA
	MA	MB	MB	B	M	A
	A	MB	MB	MB	B	M
	M	MB	MB	MB	MB	B
	B	MB	MB	MB	MB	MB

RIESGO RESIDUAL

PROBABILIDAD

[S] proteger el servicio de copias de respaldo, en cuanto a que esta disponibilidad (M) posible.
[S.A] Asegurar la disponibilidad de la aplicación para realizar las copias de respaldo, unidad de almacenamiento (disco duro externo), personal que ejecuta el proceso y la información a respaldar. (M) posible

[SS] Aceptación y puesta en operación del proceso de respaldo, autenticación y confidencialidad (M) posible

IMPACTO
[S] proteger el servicio de copias de respaldo, en cuanto a que esta disponibilidad (M) medio.
[S.A] Asegurar la disponibilidad de la aplicación para realizar las copias de respaldo, unidad de almacenamiento (disco duro externo), personal que ejecuta el proceso y la información a respaldar. (M) medio
[SS] Aceptación y puesta en operación del proceso de respaldo, autenticación y confidencialidad (MB) muy bajo

		Probabilidad				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 18. Riesgo residual 1

[P] Personal	
Código: 00002	**Nombre:** Personal que realiza el respaldo
Tipo: Activo Secundario	
Descripción: Personal del área de soporte a cargo de realizar el proceso copias de respaldo	
Propiedad: Son las características o atributos que hacen valioso el activo, estas son: Confidencialidad y Autenticación.	
Valoración: Confidencialidad: Extremo (10) Autenticación: Medio (5)	
Unidad / Persona Responsable: Soporte de informática	
Ubicación: Departamento de informática	
Cantidad: 1 persona	
DEGRADACION **Salvaguardas:** **[PS] Gestión del personal (efectuar las gestiones para la formación y el personal de contingencia para ejecutar el proceso de respaldo de forma eficiente). (M) Posible** **[PS.AT] Formación y concienciación al personal del proceso de copias de respaldos. (M) Posible** **[PS. A] Asegurarse de la disponibilidad del personal para la ejecución del proceso de**	

copias de respaldo. (M) Posible

Valor		Criterios	
MA	MUY ALTO	Casi seguro	Fácil
A	ALTO	Muy alto	Medio
M	MEDIO	Posible	Difícil
B	BAJO	Poco probable	Muy difícil
MB	MUY BAJO	Muy raro	Extremadamente difícil

PROBABILIDAD

[PS] Gestión del personal (efectuar las gestiones para la formación y el personal de contingencia para ejecutar el proceso de respaldo de forma eficiente). (M) Posible
[PS.AT] Formación y concienciación al personal del proceso de copias de respaldos. (M) Posible
[PS. A] Asegurarse de la disponibilidad del personal para la ejecución del proceso de copias de respaldo. (M) Posible

Valor			Criterios de probabilidad Residual
MA	Seguro	100	Muy frecuente (a diario)
A	Probable	10	Frecuentemente (semanalmente)
M	Posible	1	Normal (mensualmente)
B	Poco probable	1/10	Poco frecuente (una vez al año)
MB	Muy raro	1/100	Muy poco frecuente (cada varios años)

IMPACTO

Valoración:
Confidencialidad: Extremo (10)
Autenticación: Medio (5)

DEGRADACION:
[PS] Gestión del personal (efectuar las gestiones para la formación y el personal de contingencia para ejecutar el proceso de respaldo de forma eficiente). **(M) Posible**
[PS.AT] Formación y concienciación al personal del proceso de copias de respaldos**. (M) Posible**
[PS. A] Asegurarse de la disponibilidad del personal para la ejecución del proceso de copias de respaldo**. (M) Posible**

IMPACTO:

[PS] Gestión del personal (efectuar las gestiones para la formación y el personal de contingencia para ejecutar el proceso de respaldo de forma eficiente). **(M) MEDIO**
[PS.AT] Formación y concienciación al personal del proceso de copias de respaldos**. (M) MEDIO**
[PS. A] Asegurarse de la disponibilidad del personal para la ejecución del proceso de copias de respaldo**. (M) MEDIO**

[S] PERSONAL		

IMPACTO		DEGRADACION				
		1/100% (MB)	1/10% (B)	1% (M)	10% (A)	100% (MA)
VALOR DEL ACTIVO	EX	MB	B	M	A	MA
	MA	MB	MB	B	M	A
	A	MB	MB	MB	B	M
	M	MB	MB	MB	MB	B
	B	MB	MB	MB	MB	MB

RIESGO

PROBABILIDAD

[PS] Gestión del personal (efectuar las gestiones para la formación y el personal de contingencia para ejecutar el proceso de respaldo de forma eficiente). **(M) Posible**

[PS.AT] Formación y concienciación al personal del proceso de copias de respaldos**. (M) Posible**

[PS. A] Asegurarse de la disponibilidad del personal para la ejecución del proceso de copias de respaldo**. (M) Posible**

IMPACTO:

[PS] Gestión del personal (efectuar las gestiones para la formación y el personal de contingencia para ejecutar el proceso de respaldo de forma eficiente). **(M) MEDIO**

[PS.AT] Formación y concienciación al personal del proceso de copias de respaldos**. (M) MEDIO**

[PS. A] Asegurarse de la disponibilidad del personal para la ejecución del proceso de copias de respaldo**. (M) MEDIO**

RIESGO RESIDUAL:

[PS] Gestión del personal (efectuar las gestiones para la formación y el personal de contingencia para ejecutar el proceso de respaldo de forma eficiente). **(M) APRECIABLE**

[PS.AT] Formación y concienciación al personal del proceso de copias de respaldos**. (M) APRECIABLE**

[PS. A] Asegurarse de la disponibilidad del personal para la ejecución del proceso de copias de respaldo**. (M) APRECIABLE**

RIESGO		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 19. Riesgo residual 2

[Media] Soporte de información	
Código: 00003	**Nombre:** disco duro externo y aplicación para realizar el respaldo

Tipo: Activo Secundarios

Descripción: Disco duro externo que almacena el respaldo de la información y la aplicación con la que se realiza el proceso de copiado de los datos e información.

Propiedad: Son las características o atributos que hacen valioso ambos activos, estas son para la unidad de disco duro: Disponibilidad.
Y para la aplicación que realiza la copia de respaldo: Disponibilidad y Autenticación

Valoración:

- **unidad de disco duro**:

Disponibilidad: medio (5) daño importante

- **aplicación que realiza la copia de respaldo**:

Disponibilidad: Extremo (10) daño extremadamente grave

Unidad / Persona Responsable: Soporte de Informática

Ubicación: Departamento de Informática

Cantidad: 1 disco duro y una licencia de la aplicación

Salvaguardas:

[MP] protección del disco duro externo. Disponibilidad (M) Posible
[MP. A] asegurar la disponibilidad del disco externo y la licencia de la aplicación para el respaldo de los datos**. Disponibilidad** (M) Posible
[MP.clean.end] limpieza de contenido al reciclar el disco duro. **Disponibilidad** (M) Posible

Valor		Criterios	
MA	MUY ALTO	Casi seguro	Fácil
A	ALTO	Muy alto	Medio
M	MEDIO	Posible	Difícil
B	BAJO	Poco probable	Muy difícil
MB	MUY BAJO	Muy raro	Extremadamente difícil

PROBABILIDAD RESIDUAL

[MP] protección del disco duro externo. Disponibilidad (M) Posible
[MP. A] asegurar la disponibilidad del disco externo y la licencia de la aplicación para el respaldo de los datos**. Disponibilidad** (M) Posible
[MP.clean.end] limpieza de contenido al reciclar el disco duro. **Disponibilidad** (M) Posible

Valor			Criterios de probabilidad Residual
MA	Seguro	100	Muy frecuente (a diario)
A	Probable	10	Frecuentemente (semanalmente)
M	Posible	1	Normal (mensualmente)
B	Poco probable	1/10	Poco frecuente (una vez al año)
MB	Muy raro	1/100	Muy poco frecuente (cada varios años)

IMPACTO RESIDUAL

DEGRADACIÓN
[MP] protección del disco duro externo. Disponibilidad (M) Posible
[MP. A] asegurar la disponibilidad del disco externo y la licencia de la aplicación para el respaldo de los datos**. Disponibilidad** (M) Posible

[MP.clean.end] limpieza de contenido al reciclar el disco duro. **Disponibilidad** (M) Posible

VALORACIÓN:
unidad de disco duro:
Disponibilidad: (M) medio (5) daño importante
aplicación que realiza la copia de respaldo:
Disponibilidad: (EX) Extremo (10) daño extremadamente grave

IMPACTO:
[MP] protección del disco duro externo. (M) Medio
[MP. A] asegurar la disponibilidad del disco externo y la licencia de la aplicación para el respaldo de los datos**.** (M) Medio
[MP.clean.end] limpieza de contenido al reciclar el disco duro. (M) Medio

Nota: el impacto residual se determina como (M) Medio, en función de la característica de disponibilidad de la aplicación para realizar las copias, y para la unidad de disco duro el impacto residual es muy bajo (MB).

[MEDIA] SOPORTE DE INFORMACIÓN						
IMPACTO		**DEGRADACION**				
		1/100% (MB)	**1/10% (B)**	**1% (M)**	**10% (A)**	**100% (MA)**
VALOR DEL ACTIVO	**EX**	MB	B	M	A	MA
	MA	MB	MB	B	M	A
	A	MB	MB	MB	B	M
	M	MB	MB	MB	MB	B
	B	MB	MB	MB	MB	MB

RIESGO RESIDUAL

El riesgo residual para los activos de soporte de información se determina como apreciable (M).

IMPACTO:
[MP] protección del disco duro externo. (M) Medio
[MP. A] asegurar la disponibilidad del disco externo y la licencia de la aplicación para el respaldo de los datos**.** (M) Medio
[MP.clean.end] limpieza de contenido al reciclar el disco duro. (M) Medio

PROBABILIDAD RESIDUAL

[MP] protección del disco duro externo. Disponibilidad (M) Posible
[MP. A] asegurar la disponibilidad del disco externo y la licencia de la aplicación para el respaldo de los datos**. Disponibilidad** (M) Posible
[MP.clean.end] limpieza de contenido al reciclar el disco duro. **Disponibilidad** (M) Posible

RIESGO		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 20. Riesgo residual 3

[D] Datos	
Código: 00004	**Nombre:** Datos a respaldar
Tipo: Activo Secundario	
Descripción: Todos los datos e información de la CCIES que se respalda incluyendo contabilidad, sistemas/aplicaciones, transacciones con afiliados.	
Propiedad: Características o atributos que hacen valioso el activo datos a respaldar, estas son Disponibilidad, Integridad, Confidencialidad y Autenticación.	
Valoración Disponibilidad: Extremo (10) daño extremadamente grave Integridad: Extremo (10) daño extremadamente grave Confidencialidad: Extremo (10) daño extremadamente grave Autenticación: Extremo (10) daño extremadamente grave	
Unidad / Persona Responsable: Soporte de Informática	
Ubicación: Centro de datos	
Salvaguardas: **[D] Protección de las copias de seguridad: disponibilidad, (M)** **[D.A) efectuar las copias de seguridad: disponibilidad, (M)** **[D.I] asegurar la integridad de los datos respaldados realizando verificaciones periódicas de la funcionalidad del respaldo: integridad, (B)**	

Valor		Criterios degradación Residual	
MA	MUY ALTO	Casi seguro	Fácil
A	ALTO	Muy alto	Medio
M	MEDIO	Posible	Difícil
B	BAJO	Poco probable	Muy difícil
MB	MUY BAJO	Muy raro	Extremadamente difícil

CRITERIOS DE VALORACIÓN PROBABILIDAD RESIDUAL

Salvaguardas:

[D] Protección de las copias de seguridad: disponibilidad, Normal (M)
[D.A) efectuar las copias de seguridad: disponibilidad, frecuentemente (A)
[D.I] asegurar la integridad de los datos respaldados realizando verificaciones periódicas de la funcionalidad del respaldo: integridad, (B)

Valor		Criterios de probabilidad Residual
MA Seguro	100	Muy frecuente (a diario)
A Probable	10	Frecuentemente (semanalmente)
M Posible	1	Normal (mensualmente)
B Poco probable	1/10	Poco frecuente (una vez al año)
MB Muy raro	1/100	Muy poco frecuente (cada varios años)

Impacto residual

<u>Degradación residual:</u>
[D] Protección de las copias de seguridad: disponibilidad, (M)
[D.A) efectuar las copias de seguridad: disponibilidad, (M)
[D.I] asegurar la integridad de los datos respaldados realizando verificaciones periódicas de la funcionalidad del respaldo: integridad, (B)

Valor del activo: DATOS

Disponibilidad: Extremo (10) daño extremadamente grave
Integridad: Extremo (10) daño extremadamente grave
Confidencialidad: Extremo (10) daño extremadamente grave
Autenticación: Extremo (10) daño extremadamente grave

El impacto residual es medio para el activo secundario datos se determina como

[D] DATOS						
IMPACTO		DEGRADACION				
		1/100% (MB)	1/10% (B)	1% (M)	10% (A)	100% (MA)
VALOR DEL ACTIVO	EX	MB	B	M	A	MA
	MA	MB	MB	B	M	A
	A	MB	MB	MB	B	M
	M	MB	MB	MB	MB	B
	B	MB	MB	MB	MB	MB

Riesgo residual

<u>Probabilidad residual</u>:

[D] Protección de las copias de seguridad: disponibilidad, Normal (M)

[D.A) efectuar las copias de seguridad: disponibilidad, frecuentemente (A)
[D.I] asegurar la integridad de los datos respaldados realizando verificaciones periódicas de la funcionalidad del respaldo: integridad, (B)

<u>Impacto residual</u>:

[D] Protección de las copias de seguridad: (M) medio
[D.A) efectuar las copias de seguridad: (M) Medio
[D.I] asegurar la integridad de los datos respaldados realizando verificaciones periódicas de la funcionalidad del respaldo: (B) Bajo

Riesgo residual

Riesgo		Probabilidad				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Resultado de la estimación del riesgo residual:

[D] Protección de las copias de seguridad: (M) apreciable
[D.A) efectuar las copias de seguridad: (A) grave
[D.I] asegurar la integridad de los datos respaldados realizando verificaciones periódicas de la funcionalidad del respaldo: (B) bajo

Tabla 21. Riesgo residual 4

El análisis de los resultados del riesgo residual se determina como grave la falta de disponibilidad de las copias de seguridad por lo que se recomienda asumir el riesgo y establecer controles para su realización como los que se citan a continuación:

- Sistematizar el proceso de respaldo
- Realizar respaldos de forma remota
- Aumentar la frecuencia de los respaldos
- Comprimir los archivos copiados para ahorrar espacio
- Cifrar la información

CAPITULO VI. CONCLUSIONES Y RECOMENDACIONES

- Los riesgos de TI afectan en todos los niveles de la estructura organizacional de la CCIES, en otras palabras, a todas las unidades de negocio y en consecuencia a sus operaciones y procesos de dichas unidades, por lo que es importante y necesario que sean evaluados.

- La CCIES como entidad que resguarda y administra información de todos sus afiliados a nivel nacional, como de sus proyectos, necesita gestionar los riesgos de TI, que ayuden a tomar decisiones de negocio con conciencia del riesgo e integrar dicha gestión a la organización y lograr comprender que el riesgo de una unidad, Gerencia o sistema puede implicar un riesgo que no se acepta en otra Gerencia o sistema.

- Para que la CCIES pueda implementar el proyecto propuesto y abordar los riesgos de TI, aplicando las medidas adecuadas y oportunamente; es necesario crear una estructura funcional para la gestión de riesgos de tecnología, un comité de riesgo, una política para la gestión de dichos riesgos y asigne funciones de cumplimiento del control de los riesgos a la unidad de Auditoria.

CAPITULO VII. GLOSARIO DE TERMINOS

Aceptación del Riesgo: Si el riesgo está dentro de la tolerancia de la organización a si el costo de mitigar el riesgo es mayor que la pérdida potencial, la organización puede asumir dicho riesgo y absorber cualquier pérdida que ocurra

Activo: Algo de valor tangible o intangible que vale la pena proteger, incluidas las personas, la información, la infraestructura, las finanzas y la reputación.

Amenaza: Todo aquello que pueda perjudicar un activo de manera tal que ocasione daños. Causa potencial de un incidente indeseado (ISO/IEC 13335).

Análisis de Impacto: Estudio que se lleva a cabo para priorizar la criticidad de los recursos de información para la organización sobre la base de los costos (consecuencias) de eventos adversos.

Análisis de Riesgo: 1. Un proceso por el cual se estiman la frecuencia y la magnitud de los escenarios de riesgo de TI. 2. Los pasos iniciales de la gestión de riesgos: analizar el valor de los activos para la empresa, identificar las amenazas a esos activos y evaluar cuán vulnerable es cada activo para esas amenazas.

Apetito de Riesgo: Magnitud del riesgo, a nivel gerencial, que una entidad está dispuesta a aceptar en para cumplir su misión.

Continuidad del Negocio: Prevención, mitigación y recuperación de una interrupción.

Control: Medio de gestionar el riesgo, que incluye políticas, procedimientos, directrices, prácticas o estructuras organizativas de carácter administrativo, técnico, jurídico o de gestión.

Cuadro de Matriz RACI: ilustra quien responde, quien rinde cuentas, a quien se consulta y a quién se informa dentro del marco de la organización.

Escenario de Riesgo: Descripción de un evento que puede provocar un impacto en el negocio.

Estándar: Requisito obligatorio, código de práctica o especificación aprobada por una organización externa reconocida, como la Organización Internacional de Normalización (ISO).

Estimación del Riesgo: Proceso de comparación del riesgo estimado con criterios determinados para establecer la magnitud del riesgo (ISO/IEC Guía 73:2002).

Evaluación del Impacto: Evaluación de posibles consecuencias de un riesgo.

Evaluación del riesgo: Un proceso utilizado para identificar y evaluar el riesgo y sus efectos potenciales. Nota de alcance: las evaluaciones de riesgos se utilizan para identificar aquellos elementos o áreas que presentan el mayor riesgo, vulnerabilidad o exposición a la empresa para su inclusión en el plan anual de auditoría de SI.

Evento: Algo que ocurre en un lugar y un momento determinados.

Evento de Amenaza: Todo evento en el que un elemento o actor de amenaza actúe contra un activo de manera tal que pueda causar daños en forma directa.

Evento de Pérdida: Todo evento en el que una amenaza provoca una pérdida.

Evitar el Riesgo: Proceso que se utiliza para evitar sistemáticamente el riesgo, que constituye un enfoque de la gestión de riesgo.

Factor de Riesgo: Condición que puede influir en la frecuencia o magnitud y en última instancia, en el impacto de negocio de los eventos y escenarios relacionados con la TI.
Frecuencia: Medida de la cantidad de eventos que ocurren a lo largo de un período de tiempo determinado.
Gerencia: Sección de la empresa que planifica, ejecuta y monitorea las actividades de acuerdo con las directivas establecidas por el gobierno para alcanzar los objetivos de la empresa.
Gestión de riesgo: 1. Las actividades coordinadas para dirigir y controlar una empresa con respecto al riesgo Nota de alcance: En el Estándar Internacional, el término "control" se utiliza como sinónimo de "medida". (Guía ISO / IEC 73: 2002) 2. Uno de los objetivos de gobernanza. Implica reconocer el riesgo; evaluar el impacto y la probabilidad de ese riesgo; y desarrollar estrategias, tales como evitar el riesgo, reducir el efecto negativo del riesgo y / o transferir el riesgo, gestionarlo dentro del contexto del apetito de riesgo de la empresa.
Identificación de Riesgos: Proceso mediante el cual se determinan y documentan los riesgos que enfrenta una organización, se basa en el reconocimiento de amenazas, vulnerabilidades, activos y controles del entorno operativo de dicha organización.
Impacto: Magnitud de pérdida provocada por una amenaza que explota.
Incidente: Todo evento que no es parte del normal funcionamiento de un servicio y que provoca, o puede provocar una interrupción de ese servicio o una reducción de su calidad.
Incidente relacionado con TI: Un evento relacionado con TI, que causa un impacto comercial operacional, de desarrollo y / o estratégico.
Infraestructura de TI: Conjunto de hardware, software y servicios que se integran a los activos de TI de la empresa.
Magnitud: medida de la gravedad potencial de la pérdida o ganancia potencial en eventos o escenarios concretos.
Mapa de riesgo: Una herramienta (gráfica) para clasificar y mostrar el riesgo por rangos definidos para frecuencia y magnitud.
Marco: Estructura generalmente aceptada y orientada a los procesos de negocio, que establece un lenguaje común y permite procesos de negocio repetibles.
Mitigación del riesgo: Gestión de riesgo mediante el uso de contramedidas y controles.
No repudio: Garantía que una parte no puede negar haber originado datos luego de haberlo hecho, disposición de prueba de la integridad y el origen de los datos y de que estos pueden ser verificados por un tercero.
Riesgo: Combinación de la probabilidad de un evento y sus consecuencias ISO/IEC 73).
Riesgo de TI: Riesgo de negocio asociado con el uso, la propiedad, lo operación, la intervención, la influencia y la adopción de TI en una organización.
Riesgo Inherente: Nivel de riesgo o exposición sin tomar en cuenta las medidas que la dirección adopta o puede adoptar (como la implementación de controles).

Riesgo residual: El riesgo remanente, después de implementar una respuesta de riesgo.
Tolerancia al riesgo: El nivel aceptable de variación que la administración está dispuesta a permitir para cualquier riesgo particular a medida que la empresa persigue sus objetivos.
Transferencia del riesgo: El proceso de asignar riesgos a otra empresa, generalmente mediante la compra de una póliza de seguro o mediante la contratación externa del servicio.
Valor de un Activo: El valor de un activo está sujeto a diversos factores, entre ellos, el valor para la organización y para sus competidores. Los activos pueden valorar de acuerdo con lo que otro pagaría por él, o con lo que vale para la empresa.

REFERENCIA BIBLIOGRAFICA

[1] Antonio Huerta, Introducción al Análisis de Riesgos: http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

[2]Catalina Coronel, 2013, METODOLOGÍA DE EVALUACIÓN DEL GOBIERNO, RIESGOS Y CUMPLIMIENTO DE LA TECNOLOGÍA DE INFORMACIÓN EN INSTITUCIONES DEL SISTEMA FINANCIERO ECUATORIANO (Tesis de Grado)

[3]Gobierno de España, 2012, MAGERIT Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

[4] ISACA, COBIT 5, Un marco de Negocios para el Negocio para el Gobierno y la Gestión de la Empresa cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf

[5] ISACA, Manual de Preparación al examen CRISC 2015

[6] Jesús M. Consuegra Gutiérrez, (2017, mayo), Guía para la gestión de los riesgos tecnológicos para las empresas adherentes al proceso APELL del D.E.I.P Barranquilla

[7] Pablo Caneo G., 2015, CIGRAS 2015 Caso de Éxito COBIT 5. Una experiencia práctica

[8] NTS ISO/IEC 31000:2018 Gestión del Riesgo – Directrices

[9] NTS ISO/IEC 27001:2013 Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requerimientos.

[9] http://www.laboratorioti.com/2016/02/22/ticcionario-una-matriz-raci-usarla/

[10]https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Riesgos%20TI%20%20Servicios%20Financieros%20(ok).pdf

[11] https://revista.seguridad.unam.mx/numero-15/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-ii-gobierno-de-ti-y-riesgos

ANEXO I. ACTIVOS

CATALOGO DE ACTIVOS

ACTIVO	DESCRIPCIÓN
[A] Arquitectura del sistema	Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.
[D] Datos / Información	La información es un activo abstracto que es almacenado en equipos o soportes de información (normalmente agrupado como archivos o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. Ejemplos: [backup] copias de respaldo, [contraseña] credenciales (ej. contraseñas): [acl] datos de control de acceso [source] código fuente [exe] código ejecutable [test] datos de prueba.
[S] Servicios	Servicios prestados por el sistema a usuarios. Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización.
[SW] Software - Aplicaciones informáticas	Programas, aplicativos, desarrollos, etc.
[HW] Equipo informático (hardware)	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción. Ejemplo: impresoras y servidores de impresión, equipos que se instalan entre dos zonas de confianza, equipamiento necesario para transmitir datos: routers, módems, etc.
[COM] Redes de comunicaciones	Instalaciones dedicadas como servicios de comunicaciones contratados a terceros, son medios de transporte que llevan datos de un sitio a otro.
[Media] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[P] Personal	[adm] administradores de sistemas [com] administradores de comunicaciones

	[dba] administradores de BBDD [sec] administradores de seguridad [des] desarrolladores / programadores [sub] subcontratas [prov] proveedores

Tabla 22. Catálogo de Activos

DIMESION DE LOS ACTIVOS

Activos primarios

ACTIVO / DIMENSION	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD
[S]	✗	✓	✓	✓

Tabla 23. Dimensión de los activos primarios

Activos secundarios

ACTIVO / DIMENSION	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD
[D]	✓	✓	✓	✗
[SW]	✗	✓	✓	✓
[P]	✓	✗	✗	✓

Tabla 24. Dimensión de los activos secundarios

FICHA DE ACTIVOS

[SW] Software - Aplicaciones informáticas	
Código: 00001	**Nombre:** Nombre del Activo
Tipo: Activos Primarios / Secundarios	
Descripción: Considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos	
Propiedad: Son las características o atributos que hacen valioso un activo, estas son Disponibilidad, Integridad, Confidencialidad y Autenticación.	
Valoración:	
Unidad / Persona Responsable:	
Ubicación:	
Cantidad:	

Tabla 25. Ficha de Activos

ANEXO II. AMENAZAS

CATALOGO DE AMENZAS

La siguiente tabla es tomada de las amenazas de MAGERIT versión 3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

AMENAZAS	DETALLE DE AMENAZAS
[N] Desastres naturales	[N.1] Fuego, [N.2] Daños por agua, [N.*] Desastres naturales.
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.3] Errores de monitorización (log), [E.4] Errores de configuración, [E.5] Difusión de software dañino, [E.6] Alteración accidental de la información, [E.7] Destrucción de información, [E.8] Fugas de información, [E.9] Errores de mantenimiento / actualización de programas (software), [E.10] Errores de mantenimiento / actualización de equipos (hardware), [E.11] Caída del sistema por agotamiento de recursos, [E.12] Indisponibilidad del personal.
[A] Ataques intencionados	[A.1] Manipulación de los registros de actividad (log), [A.2] Manipulación de la configuración, [A.3] Suplantación de la identidad del usuario, [A.4] Abuso de privilegios de acceso. [A.5] Acceso no autorizado, [A.6] Análisis de tráfico, [A.7] Repudio, [A.8] Interceptación de información (escucha), [A.9] Modificación deliberada de la información, [A.10] Destrucción de información, [A.11] Divulgación de información, [A.12] Manipulación de programas, [A.13] Manipulación de los equipos, [A.14] Denegación de servicio, [A.15] Indisponibilidad del personal, [A.16] Ingeniería social.

Tabla 26. Catálogo de amenazas

FICHA DE AMENAZAS

[código] Nombre de la amenaza	
Activos: Activos que se pueden ver afectados por este tipo de amenaza.	**Dimensiones:** Dimensiones de los activos que se ven afectadas por este tipo de amenaza.
Probabilidad: La probabilidad de ocurrencia de la amenaza	
Degradación: El grado de degradación que causaría si se materializa la amenaza	
Descripción: Información detallada de lo que puede ocurrir a los activos afectados.	

Tabla 27. Ficha de amenazas

ANEXO III. IMPACTO Y RIESGO POTENCIAL

ESTIMACION DEL IMPACTO RESIDUAL

[Código] Nombre del Activo				
IMPACTO		**DEGRADACION**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 28. Estimación del impacto por activo

ESTIMACION DEL RIESGO RESIDUAL

[Código] Nombre del Activo						
RIESGO		**PROBABILIDAD**				
		MB	**B**	**M**	**A**	**MA**
IMPACTO	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 29. Estimación del riesgo por activo

ANEXO IV. CONTROLES

CATALOGO DE CONTROLES

Los objetivos de control y controles listados en la Tabla A.1 corresponden a los listados en el Anexo A de la ISO/IEC 27001:2013

Controles para el tratamiento del riesgo

A.5 Política de seguridad de la información		
A.5.1 Gestión de la dirección para la seguridad de la información Objetivo: Proporcionar directrices y apoyo para la seguridad de la información en concordancia con los requerimientos del negocio, leyes y regulaciones pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	Control Un conjunto de políticas de seguridad de la información debe ser definido y aprobado por la Dirección, publicarlo y comunicarlo a todos los empleados y entidades externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Control Las políticas para la seguridad de la información deben revisarse a períodos planificados o siempre que se produzcan cambios significativos, para asegurar que se mantenga su continuidad, idoneidad, adecuación y efectividad.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Control Todas las responsabilidades de la seguridad de la información deben estar definidas y asignadas.

A.6.1.2	Segregación de funciones	Control Las funciones conflictivas y las áreas de responsabilidad deben ser segregadas para reducir las oportunidades de modificaciones o uso no autorizado o mal intencionado de los activos de la organización.
A.6.1.3	Contacto con autoridades	Control Deben mantenerse los contactos adecuados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de especial interés	Control Se deben mantener contactos apropiados con los grupos de especial interés u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Control La seguridad de la información debe ser tratada en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2 Dispositivos móviles y trabajo remoto		
Objetivo: Asegurar la seguridad del trabajo remoto y el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	Control Una política y medidas de soporte de seguridad deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Trabajo remoto	Control Una política y medidas de soporte de seguridad deben ser implementadas para proteger la información accedida, procesada o almacenada en sitios de trabajo remoto.
A.7 Seguridad de los recursos humanos		
A.7.1 Antes del empleo Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y sean idóneos para los roles para los cuales se les considera.		

A.7.1.1	Selección de personal	Control Los controles de verificación de los antecedentes de todos los candidatos para el empleo deben llevarse a cabo en concordancia con las leyes, regulaciones y normas de ética pertinentes y, deben ser proporcionales al requerimiento del negocio, la clasificación de la información a ser accedida y los riesgos percibidos.
A.7.1.2	Términos y condiciones de empleo	Control Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las responsabilidades de la organización para la seguridad de la información.
A.7.2 Durante el empleo Objetivo: Asegurar que todos los empleados y contratistas estén conscientes de cumplir con sus responsabilidades de la seguridad de la información.		
A.7.2.1	Responsabilidades de la Dirección	Control La Dirección debe requerir que los empleados y contratistas apliquen la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Capacitación, educación y concientización sobre la seguridad de la información	Control Todos los empleados de la organización y, cuando sea pertinente, los contratistas, deben recibir una apropiada concientización, capacitación y actualización periódica de las políticas y procedimientos organizacionales, que sean relevantes a su función laboral.
A.7.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal y comunicado de forma que se tomen acciones en contra de empleados que han cometido una violación en la seguridad de la información.
A.7.3 Terminación y cambio del empleo Objetivo: Proteger los intereses de la organización como parte de un proceso de terminación o cambio de empleo.		

A.7.3.1	Responsabilidades de terminación o cambio de empleo	Control Deben ser definidas las responsabilidades y funciones de la seguridad de la información que permanezcan validas después de una terminación o cambio de empleo, comunicadas y remarcadas al empleado o contratista.
A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos Objetivo: Identificar los activos organizacionales y definir las apropiadas responsabilidades de protección.		
A.8.1.1	Inventario de activos	Control Activos asociados con información e instalaciones de procesamiento de la información deben ser identificados y un inventario de estos activos debe ser levantado y mantenido.
A.8.1.2	Propiedad de los activos	Control Los activos dentro del inventario deben ser asignados.
A.8.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información, los activos asociados y las instalaciones para procesamiento de la información.
A.8.1.4	Devolución de los activos	Control Todos los empleados y usuarios externos deben devolver todos los activos de la organización que se encuentran en su posesión una vez dada la terminación de su empleo, contrato o acuerdo.
A.8.2 Clasificación de la información Objetivo: Asegurar que la información reciba un nivel apropiado de protección en concordancia con su importancia para la organización		
A.8.2.1	Clasificación de la información	Control La información debe ser clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad a modificaciones o divulgación no autorizada.

A.8.2.2	Etiquetado de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar la información en concordancia con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Control Se debe desarrollar e implementar procedimientos para manejo de activos en concordancia con el esquema de clasificación de información adoptado por la organización.
A.8.3 Manejo de medios Objetivo: Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de información almacenada en medios.		
A.8.3.1	Gestión de los medios removibles	Control Se deben implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de medios	Control Se deben eliminar los medios de manera segura cuando ya no son requeridos utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Control Medios que contengan información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante su transporte.
A.9 Control de acceso		
A.9.1 Requerimiento del negocio para el control de acceso Objetivo: Limitar el acceso a la información y a instalaciones de procesamiento de la información.		
A.9.1.1	Política del control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basada en los requerimientos de seguridad de la información y del negocio.
A.9.1.2	Acceso a redes y servicios de red	Control Se debe proveer a los usuarios únicamente con acceso a la red y servicios de red que hayan sido específicamente autorizados.

A.9.2 Gestión del acceso de usuarios Objetivo: Asegurar el acceso autorizado a los usuarios y prevenir el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y anulación de usuarios	Control Para habilitar la asignación de derechos de acceso se debe implementar un procedimiento formal para la creación y anulación de usuarios.
A.9.2.2	Provisión de accesos de usuarios	Control Se debe implementar un proceso formal de provisión de accesos de usuario para asignar o revocar derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.
A.9.2.3	Gestión de privilegios de derechos de acceso	Control Se debe restringir y controlar la asignación y uso de los privilegios de derechos de acceso.
A.9.2.4	Gestión de la información de autenticación secreta de los usuarios	Control Se debe controlar a través de un proceso formal de gestión la asignación de información de autenticación secreta.
A.9.2.5	Revisión de los derechos de acceso	Control Los dueños de los activos deben revisar periódicamente los derechos de acceso de los usuarios.
A.9.2.6	Remover o ajustar los derechos de acceso	Control Se deben remover los derechos de acceso de todos los empleados y usuarios externos a la información e instalaciones de procesamiento de la información una vez dada la terminación de su empleo, contrato o acuerdo, o ser ajustados cuando se dé un cambio.
A.9.3 Responsabilidades del usuario Objetivo: Hacer responsables a los usuarios por salvaguardar su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	Control Se debe requerir a los usuarios seguir las prácticas de la organización en el uso de la información de autenticación secreta.

A.9.4 Control de acceso a sistemas y aplicaciones Objetivo: Prevenir el acceso no autorizado a sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	Control Se debe restringir el acceso a la información y a funcionalidades de los sistemas de aplicación en concordancia con la política de control de acceso.
A.9.4.2	Procedimientos seguros de inicio de sesión	Control Cuando sea requerido por la política de control de acceso, se deben controlar por un procedimiento seguro de inicio de sesión el acceso a los sistemas y aplicaciones.
A.9.4.3	Sistema de gestión de la contraseña	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	Control Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de sobrescribir los controles de aplicaciones y sistema.
A.9.4.5	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.
A.10 Criptografía		
A.10.1 Controles criptográficos Objetivo: Asegurar el apropiado y efectivo uso de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	Control Se debe desarrollar e implementar una política sobre el uso, protección y duración de las llaves criptográficas durante todo el ciclo de vida.

A. 11 Seguridad física y ambiental		
A.11.1 Áreas seguras Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones de procesamiento de la información y a la información de la organización.		
A.11.1.1	Perímetro de seguridad física	Control Se deben definir y utilizar perímetros de seguridad para proteger áreas que contienen información, ya sea sensitiva o crítica, e instalaciones de procesamiento de la información.
A.11.1.2	Controles de entrada físicos	Control Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A.11.1.3	Seguridad de oficinas, habitaciones e instalaciones	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar procedimientos para trabajar en áreas seguras.
A.11.1.6	Áreas de carga y descarga	Control Se deben controlar los puntos de acceso como las áreas de carga y descarga y otros puntos donde personas no autorizadas puedan ingresar a las instalaciones, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.11.2 Equipo Objetivo: Prevenir la pérdida, daño, robo o exposición de los activos y la interrupción de las operaciones de la organización.		

A.11.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado y protegido para reducir los riesgos de amenazas y peligros ambientales, y de las oportunidades de accesos no autorizados.
A.11.2.2	Herramientas de soporte	Control El equipo debe ser protegido contra fallas de energía y otras interrupciones causadas por fallas en las herramientas de soporte.
A.11.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que transportan datos o soportan servicios de información, deben ser protegidos de intercepción, interferencia o daño.
A.11.2.4	Mantenimiento de equipo	Control El equipo debe recibir un correcto mantenimiento para asegurar su continuidad, disponibilidad e integridad.
A.11.2.5	Retiro de activos	Control El equipo, información o software no debe ser extraído de las instalaciones sin previa autorización.
A.11.2.6	Seguridad del equipo y activos fuera de las instalaciones	Control Al trabajar con equipos y activos fuera de las instalaciones de la organización, se deben aplicar medidas de seguridad considerando los riesgos que esto implica.
A.11.2.7	Seguridad en la reutilización o eliminación de equipos	Control Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y el software con licencia hayan sido eliminados o sobrescrito con seguridad antes de su reutilización o eliminación.
A.11.2.8	Equipo desatendido de usuario	Control Los usuarios deben asegurarse de que el equipo desatendido tiene protección apropiada.

A.11.2.9	Política de escritorio y pantalla limpia	Control Se debe adoptar una política de escritorio limpio para documentos y medios de almacenamiento removibles y una política de pantalla limpia en las instalaciones de procesamiento de la información.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.		
A.12.1.1	Procedimientos de operación documentados	Control Los procedimientos de operación deben documentarse y estar disponibles a todos los usuarios que lo necesiten.
A.12.1.2	Gestión de cambios	Control Cambios en la organización, procesos de negocios, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de la capacidad	Control El uso de los recursos debe ser monitoreado, optimizado y se deben realizar proyecciones de la capacidad futura necesaria para asegurar el desempeño requerido por el sistema.
A.12.1.4	Separación de los ambientes de desarrollo, prueba y producción	Control Los ambientes de desarrollo, prueba y producción, deben estar separados para reducir los riesgos de acceso no autorizado o cambios en el ambiente en producción.
A.12.2 Protección contra software malicioso Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra software malicioso.		

A.12.2.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse contra software malicioso, combinándolos con una apropiada concientización del usuario.
A.12.3 Copias de seguridad Objetivo: Protección contra pérdida de datos.		
A.12.3.1	Copia de seguridad de la información	Control Se debe hacer copias de seguridad de la información, software e imágenes del sistema y probarlas periódicamente de acuerdo con la política de respaldo.
A.12.4 Registro y monitoreo Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de eventos	Control Se deben producir, mantener y revisar periódicamente registros de los eventos de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la bitácora de información	Control Las instalaciones de registro y la bitácora de la información deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
A.12.4.3	Bitácoras del administrador y operador	Control Se deben llevar bitácoras de las actividades del administrador y operador del sistema y éstas deben ser protegidas y revisadas regularmente.
A.12.4.4	Sincronización de reloj	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una única fuente de tiempo de referencia.
A.12.5 Control de software operacional Objetivo: Asegurar la integridad de los sistemas operacionales		

A.12.5.1	Instalación de software en sistemas operacionales	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: Prevenir la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de vulnerabilidades técnicas	Control Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para abordar el riesgo asociado.
A.12.6.2	Restricción en la instalación de software	Control Se deben establecer e implementar reglas que rijan la instalación de software por parte de los usuarios.
A.12.7 Consideraciones en la auditoria de sistemas de información Objetivo: Minimizar el impacto de las actividades de auditoria en los sistemas en producción		
A 12.7.1	Controles de auditoria de los sistemas de información	Control Los requerimientos y actividades de auditoria que involucran los sistemas en producción deben ser cuidadosamente planificados y acordados para minimizar las interrupciones a los procesos de negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de seguridad de red Objetivo: Asegurar la protección de la información en redes y su soporte a las instalaciones de procesamiento de la información.		
A.13.1.1	Controles de red	Control Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control Mecanismos de seguridad, niveles de servicio y requisitos de la gestión de todos los servicios de red, deben ser identificados e incluidos en cualquier acuerdo de servicios de red, ya sea si estos servicios son provistos por la misma organización o se subcontratan.

A.13.1.3	Segmentación de redes	Control Se deben segmentar en redes los grupos de servicios de información, usuarios y sistemas de información.
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	Procedimientos y políticas de transferencia de información	Control Se deben establecer políticas, procedimientos y controles formales para proteger la transferencia de información a través de todos los tipos de recursos de comunicación.
A.13.2.2	Acuerdos de transferencia de información	Control Los acuerdos deben abordar la seguridad de la transferencia de información del negocio entre la organización y entidades externas.
A.13.2.3	Mensajes electrónicos	Control Se debe proteger adecuadamente la información contenida en los mensajes electrónicos.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Control Se deben identificar, revisar periódicamente y documentar los requerimientos para acuerdos de confidencialidad o no divulgación, reflejando las necesidades de la organización para la protección de la información.
A.14 Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información. Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información a través de todo su ciclo de vida. Esto también incluye los requerimientos para sistemas de información que proveen servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requerimientos de seguridad de la información	Control Los requerimientos relacionados a seguridad de la información deben ser incluidos en los requerimientos para nuevos sistemas de información, o mejoras a sistemas de información existentes.

A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Control La información involucrada en servicios de aplicación sobre redes públicas debe ser protegida de actividades fraudulentas, disputas de contrato y divulgación no autorizada y modificación.
A.14.1.3	Protección de transacciones de servicios de aplicación	Control La información involucrada en transacciones en servicios de aplicación debe ser protegida para prevenir transacciones incompletas, mal enrutamiento, alteración, divulgación, duplicación o replicación no autorizada de mensajes.
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 de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	Control Se debe establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control Los cambios a los sistemas dentro del ciclo de vida de desarrollo deben ser controlados a través del uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma operativa	Control Cuando se cambien las plataformas operativas, se debe revisar y probar las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control Se debe desalentar las modificaciones a los paquetes de software, limitándolas a cambios necesarios y todos los cambios deben ser estrictamente controlados.
A.14.2.5	Principios de ingeniería de sistemas seguros	Control Se deben establecer, documentar, mantener y aplicar principios para ingeniería de sistemas seguros en cualquier iniciativa de implementación de sistemas de información.

A.14.2.6	Ambiente de desarrollo seguro	Control Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro, para iniciativas de desarrollo e integración de sistemas que cubran todo el ciclo de vida de desarrollo.
A.14.2.7	Desarrollo subcontratado	Control La organización debe supervisar y monitorear las actividades del desarrollo subcontratado de sistemas.
A.14.2.8	Pruebas de seguridad del sistema.	Control Las pruebas de la funcionalidad de seguridad del sistema deben llevarse a cabo durante su desarrollo.
A.14.2.9	Pruebas de aceptación del sistema.	Control Se deben establecer programas de pruebas de aceptación y los criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de los datos de prueba.	Control Datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.
A.15 Relaciones con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores. Objetivo: Asegurar la protección de los activos de la organización que son accesibles por los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores.	Control Se debe de acordar con el proveedor y documentar los requerimientos de seguridad de la información, para la mitigación de los riesgos asociados con el acceso de los proveedores a los activos de la organización.

A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Control Se deben establecer y acordar todos los requerimientos de seguridad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Tecnología de información y comunicación en la cadena de suministro.	Control Los acuerdos con proveedores deben incluir los requerimientos para abordar los riesgos de seguridad de información asociados con los servicios de tecnología de comunicaciones e información y la cadena de suministro de productos.
A.15.2 Gestión del servicio de entrega del proveedor. Objetivo: Mantener un nivel acordado de seguridad de la información y el servicio de entrega alineados con los acuerdos del proveedor.		
A.15.2.1	Monitoreo y revisión de los servicios del proveedor.	Control La organización debe monitorear, revisar y auditar periódicamente el servicio de entrega del proveedor.
A.15.2.2	Gestión de cambios en los servicios del proveedor.	Control Se deben gestionar los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, teniendo en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y la reevaluación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras Objetivo: Asegurar un enfoque consistente y efectivo para la gestión de incidentes de seguridad de la información, incluyendo la comunicación en los eventos y debilidades de seguridad.		
A.16.1.1	Procedimientos y responsabilidades.	Control Se debe establecer procedimientos y responsabilidades de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

A.16.1.2	Informar sobre los eventos de seguridad de la información.	Control Los eventos de seguridad de la información deben ser informados a través de los canales de administración adecuados tan pronto como sea posible.
A.16.1.3	Informar sobre las debilidades de seguridad de la información.	Control Se debe requerir que los empleados y contratistas que utilizan los sistemas y servicios de información de la organización tomen nota e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios de la organización.
A.16.1.4	Evaluación y toma de decisión sobre los eventos de seguridad de la información.	Control Se debe evaluar los eventos de seguridad de la información y decidir si éstos se clasificarán como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información.	Control Se debe responder a los eventos de seguridad de la información en concordancia con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	Control Se debe utilizar los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia.	Control La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda ser utilizada como 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 estar incluida en los sistemas de gestión de la continuidad del negocio de la organización.		

A.17.1.1	Planeación de la continuidad de la seguridad de la información.	Control La organización debe determinar los requerimientos para seguridad de la información y la gestión de la continuidad de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	Control La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles, para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información.	Control La organización debe verificar periódicamente los controles establecidos e implementados para la continuidad de la seguridad de la información, a fin de asegurar que son válidos y efectivos durante situaciones adversas.
A.17.2 Redundancias Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información.		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información.	Control Las Instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir requerimientos de disponibilidad.
A.18 Cumplimento		
A.18.1 Cumplimiento con requerimientos legales y contractuales Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requerimiento de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y requerimientos contractuales	Control Todos los estatutos legales, regulaciones, requerimientos contractuales relevantes y el enfoque de la organización para cumplir estos requerimientos deben estar explícitamente identificados, documentados y actualizados para cada sistema de información y para la organización.

A.18.1.2	Derechos de propiedad intelectual	Control Se debe implementar procedimientos adecuados para asegurar el cumplimiento de requerimientos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y uso de productos de software propietario.
A.18.1.3	Protección de los registros	Control Se deben proteger los registros contra pérdida, destrucción, falsificación, acceso y divulgación no autorizada, de conformidad con leyes, regulaciones, contratos y requerimientos del negocio.
A.18.1.4	Privacidad y protección de información identificada como personal	Control Se debe asegurar la protección de información identificada como personal y su privacidad acorde a lo dispuesto en la legislación y la reglamentación pertinente, cuando aplique.
A.18.1.5	Regulación de los controles criptográficos	Control Los controles criptográficos deben ser utilizados en cumplimiento de todos los acuerdos, legislaciones y regulaciones pertinentes.
A.18.2 Revisiones de seguridad de la información Objetivo: Asegurar que la seguridad de la información se implemente y opere en concordancia con las políticas y procedimientos de la organización.		
A.18.2.1	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para la gestión de seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), deben ser revisados de forma independiente en periodos planificados o cuando se produzcan cambios significativos.

A.18.2.2	Cumplimiento de las políticas y normas de seguridad.	Control Los gerentes deben revisar periódicamente, dentro de su área de responsabilidad, el cumplimiento de los procedimientos y procesamiento de la información de acuerdo con las políticas de seguridad, normas y otros requerimientos de seguridad apropiados.
A.18.2.3	Revisión de cumplimiento técnico.	Control Se debe revisar periódicamente el cumplimiento de los sistemas de información con respecto a las políticas y normas de seguridad de la información de la organización.

Tabla 30. Catálogo de Controles para el tratamiento del riesgo

TIPOS DE CONTROLLES

Nombre	Descripción
[PR] prevención	Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en preproducción, segregación de tareas.
[DR] disuasión	Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente.
[EL] eliminación	Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir. Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, en general, todo lo que tenga que ver con la fortificación o bastionado, cifrado de la información, armarios ignífugos.
[IM] minimización del impacto / limitación del impacto	Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente. Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente
[CR] corrección	Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños. Véase: recuperación más abajo.

	Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes.
[RC] recuperación	Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo. Ejemplos: copias de seguridad (back-up)
[MN] monitorización	Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro. Ejemplos: registros de actividad, registro de descargas de web.
[DC] detección	Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños. Ejemplos: antivirus, IDS, detectores de incendio.
[AW] concienciación	Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación. Ejemplos: cursos de concienciación, cursos de formación.
[AD] administración	Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo. Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad.

Tabla 31. Tipos de Controles

EFICIENCIA Y MADUREZ DE LOS CONTROLES

Nivel	Factor	Significado
N0	0%	Inexistente
N1	10%	Inicial / ad hoc
N2	30%	Reproducible, pero intuitivo
N3	60%	Proceso definido
N4	80%	Gestionado y Medible
N5	100%	Optimizado

Tabla 32. Eficiencia y madurez de los controles

FICHA DE CONTROLES

[Código] Nombre del control	
Tipo: Tipo de control	
Estado: Factor	**Nivel:** Nivel de Eficiencia
Amenaza: Amenaza a la que se aplica el control	
Descripción: Descripción del control aplicado	

Tabla 33. Ficha de Controles

ANEXO V. EVALUACION DE CONTROLES

Norma	Sección	Cumplimiento	
5	**POLITICAS DE SEGURIDAD**	**0%**	
5.1	**Directrices de la Dirección en seguridad de la información**	**0%**	
5.1.1	Conjunto de políticas para la seguridad de la información	**No realizado**	0%
5.1.2	Revisión de las políticas para la seguridad de la información	**No realizado**	0%
8	**GESTION DE ACTIVOS**	**0%**	
8.1	**Responsabilidad sobre los Activos**	**0%**	
8.1.1	Inventario de activos.	**No realizado**	0%
8.1.2	Propiedad de los activos.	**No realizado**	0%
8.1.3	Uso aceptable de los activos.	**No realizado**	0%
8.1.4	Devolución de activos.	**No realizado**	0%
8.2	**Clasificación de la Información**	**0%**	
8.2.1	Directrices de clasificación.	**No realizado**	0%
8.2.2	Etiquetado y manipulado de la información.	**No realizado**	0%
8.3	**Manejo de los soportes de almacenamiento**	**0%**	
8.3.1	Gestión de soportes extraíbles.	**No realizado**	0%
8.3.2	Eliminación de soportes.	**No realizado**	0%
8.3.3	Soportes físicos en tránsito	**No realizado**	0%
9	**CONTROL DE ACCESO**	**0%**	
9.1	**Requisitos de negocio para el control de accesos**	**0%**	
9.1.1	Política de control de accesos.	**No realizado**	0%
9.1.2	Control de acceso a las redes y servicios asociados.	**No realizado**	0%
9.2	**Gestión de acceso de usuario.**	**0%**	
9.2.1	Gestión de altas/bajas en el registro de usuarios.	**No realizado**	0%
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	**No realizado**	0%
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	**No realizado**	0%

9.2.5	Revisión de los derechos de acceso de los usuarios.	**No realizado**	0%
9.2.6	Retirada o adaptación de los derechos de acceso	**No realizado**	0%
9.4	**Control de acceso a sistemas y aplicaciones**	**0%**	
9.4.1	Restricción del acceso a la información.	**No realizado**	0%
9.4.2	Procedimientos seguros de inicio de sesión.	**No realizado**	0%
9.4.3	Gestión de contraseñas de usuario.	**No realizado**	0%
9.4.4	Uso de herramientas de administración de sistemas.	**No realizado**	0%
9.4.5	Control de acceso al código fuente de los programas	**No realizado**	0%
11	**SEGURIDAD FISICA Y AMBIENTAL**	**0%**	
11.1	**Áreas Seguras**	**0%**	
11.1.1	Perímetro de seguridad física.	**No realizado**	0%
11.1.2	Controles físicos de entrada.	**No realizado**	0%
11.1.3	Seguridad de oficinas, despachos y recursos.	**No realizado**	0%
11.1.4	Protección contra las amenazas externas y ambientales.	**No realizado**	0%
11.1.5	El trabajo en áreas seguras.	**No realizado**	0%
11.1.6	Áreas de acceso público, carga y descarga	**No realizado**	0%
11.2	**Seguridad de los Equipos**	**0%**	
11.2.1	Emplazamiento y protección de equipos.	**No realizado**	0%
11.2.2	Instalaciones de suministro.	**No realizado**	0%
11.2.3	Seguridad del cableado.	**No realizado**	0%
11.2.4	Mantenimiento de los equipos.	**No realizado**	0%
11.2.5	Salida de activos fuera de las dependencias de la empresa.	**No realizado**	0%
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	**No realizado**	0%
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	**No realizado**	0%
11.2.8	Equipo informático de usuario desatendido.	**No realizado**	0%
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	**No realizado**	0%
12	**SEGURIDAD EN LA OPERATIVA**	**0%**	
12.2	**Protección contra código malicioso**	**0%**	
12.2.1	Controles contra el código malicioso.	**No realizado**	0%
12.3	**Copias de seguridad**	**0%**	
12.3.1	Copias de seguridad de la información	**No realizado**	0%
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**	**0%**	
13.1	**Gestión de la seguridad en las redes.**	**0%**	
13.1.1	Controles de red.	**No realizado**	0%
13.1.2	Mecanismos de seguridad asociados a servicios en red.	**No realizado**	0%
13.1.3	Segregación de redes.	**No realizado**	0%
13.2	**Intercambio de información con partes externas.**	**0%**	
13.2.1	Políticas y procedimientos de intercambio de información.	**No realizado**	0%
13.2.2	Acuerdos de intercambio.	**No realizado**	0%

13.2.3	Mensajería electrónica.	**No realizado**	0%
13.2.4	Acuerdos de confidencialidad y secreto	**No realizado**	0%
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**	**0%**	
14.2	**Seguridad en los procesos de desarrollo y soporte**	**0%**	
14.2.1	Política de desarrollo seguro de software.	**No realizado**	0%
14.2.6	Seguridad en entornos de desarrollo.	**No realizado**	0%
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	**No realizado**	0%

Tabla 34. Evaluación de controles

ANEXO VI. INDICE DE TABLAS

ANEXO VII. INDICE DE FIGURAS