UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

GUIA DE IMPLEMENTACION DEL AREA DE SEGURIDAD DE LA INFORMACIÓN COMO UN SERVICIO DE TI BASADO EN LAS BUENAS PRÁCTICAS DE COBIT 5, ISO 27001 E ITIL.

PARA OPTAR AL GRADO DE:

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

MG. RENE ARTURO ANGULO ARRIAZA

PRESENTADO POR:

GLENDA LISSETTE CHAVEZ LANDAVERDE

JOSE FIDEL ANTONIO GALDAMEZ CALLES

KARLA JENIFFER VIERA HERNANDEZ

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica

Agosto 2018

AGRADECIMIENTOS:

Agradezco a Dios todo poderoso por haberme regalado vida, salud, sabiduría y dedicación por permitirme alcanzar un objetivo más en mi vida como persona y profesional.

“Porque de Él, por Él y para Él son todas las cosas. A Él sea la gloria para
siempre. Amén.” Ro.
11:36 (NVI)

A mis padres y hermanos, por brindarme el apoyo y motivación día a día para continuar alcanzando mis metas, dándome fortaleza en los momentos más difíciles y confiando siempre en mí en lograr culminar este objetivo personal.

A nuestro asesor de tesis que a lo largo del desarrollo de está, nos apoyó, guio y nos brindó sus sabios consejos conforme a su experiencia para lograr alcanzar nuestra meta.

A mis compañeros, que juntos logramos hacer un buen equipo de trabajo, sin cada uno de ellos no se hubiera podido alcanzar nuestro logro en común, para culminar esta carrera la cual nos ayudó a desarrollarnos para ser mejores profesionales que necesita nuestro país.

Glenda Lissette Chávez Landaverde

AGRADECIMIENTOS:

A DIOS todo poderoso por darme la vida y permitirme satisfactoriamente culminar esta Maestría.

A mis padres (Q.D.D.G) quienes con profundo amor, esfuerzos y fe, me ayudaron en todo momento. Como hubiera deseado poder compartirlo con ellos...

A mi esposa e hijos, quienes me acompañaron, gracias por su comprensión, apoyo y aliento en el tiempo que duró este esfuerzo.

A mi hermano, por brindarme su apoyo y consejos a seguir adelante.

Agradecer de manera especial al asesor, por su valiosa colaboración y por todos los aportes brindados a nuestro grupo de trabajo, ya que fueron de gran ayuda para nuestra formación.

A la Universidad y docentes, por brindarnos conocimientos necesarios para el desarrollo de nuestra carrera

Finalmente a mis compañeras de grupo tesis y demás compañeros a quienes les agradezco su amistad y apoyo.

José Fidel Antonio Galdámez Calles

AGRADECIMIENTOS:

Agradezco primeramente a Dios por la bendición que me ha dado de tener la capacidad y los recursos para poder culminar este enorme logro, y su vez poner en mi camino personas que han sido claves en el transcurso de esta carrera, a quienes también agradezco por su apoyo, mis padres y mis hermanos, por estar presentes en cada paso que di desde el momento en que tomé la decisión de iniciar la maestría, en las noches de desvelo, es indescriptible sentir el apoyo hombro a hombro, cuando hay alguien ahí también despierto por el simple hecho de dar apoyo, ánimo y un abrazo que en más de una ocasión renovó mis energías, gracias mamá, gracias papá.

Mi novio y su familia por animarme y darme consejos que me han ayudado mucho.

Nuestro asesor de tesis que con mucho profesionalismo nos ha guiado,

corregido y animado para que este logro sea hoy una realidad. Así como también nos ha brindado sabios consejos que me han servido no solo en esta etapa como estudiante sino como profesional y persona.

Y finalmente pero no con menos importancia, a mis compañeros de tesis que desde el inicio de la carrera congeniamos y nos convertimos en equipo no para una matera, sino para toda la carrera, y hoy siendo más que un grupo de trabajo de tesis los considero mis amigos, unas grandes personas de quienes he aprendido mucho y espero poder tener la dicha de volver a trabajar juntos de nuevo.

Karla Jeniffer Viera Hernández

Contenido

1. Introducción

En la actualidad se ha observado que en el mundo entero se está concientizando sobre la seguridad de los datos, en un estudio publicado en el 2008 por US-CERT Introduction to Information Security, comenta sobre los conceptos básicos que debe de tener la seguridad que son confidencialidad, integridad y disponibilidad que debe de poseer los datos que se almacenan, al mismo tiempo hace un análisis de lo que podría suceder al no tomar las medidas correspondientes ante accesos no autorizados o copias de la información, ya que como se sabe todo lo que se encuentra en internet no es inmune ante las vulnerabilidades que se presentan hoy en día.

En otro estudio presentado por ESET titulado *Resumen de Seguridad 2017: el año de los llamados de atención*, menciona que los datos se encuentran propensos a diferentes vulnerabilidades, que cada vez se hacen más penetrantes por virus, malwares, hacking entre otros, esto hace que el registro de impactos aumente simultáneamente y se debe a que en algunas casos las empresas no se cuenta con infraestructuras seguras y antivirus o softwares actualizados que protejan los datos contra estos tipos de amenazas.

Todo esto nos hace pensar en la importancia que tiene la seguridad de la información y en nuestro país El Salvador, consideramos que con todo lo que ha ocurrido a nivel mundial en los últimos años con los avances tecnológicos se pueda brindar a las empresas una guía en la que se posea la información necesaria para la creación de un área de seguridad de información, que sería la encargada de implementar nuevas tendencias de tecnología ya sea infraestructura o software que proteja ante las diferentes amenazas que están aconteciendo contra la seguridad de los datos.

Esta guía pretende facilitar la identificación de los componentes y procesos que deben ser considerados en el área de seguridad de información, todos estos procesos se estarán basándose en las normas ISO 27001:2013 y 27002:2013, buenas prácticas de COBIT 5.0 e ITIL v3 2011 y así mediante este análisis de los tres componen poder crear una guía estándar que pueda ser adaptada según la necesidad de cada idea de negocio, que mediante la investigación de las normas estudiadas y buenas prácticas podemos sustentar la guía mediante conceptos, requisitos y procesos claves e indispensables que se deben de considerar como requisitos mínimos al momento de tener como objetivo la creación de un área de seguridad de la información en el departamento de TI.

2. Objetivo General y específicos

2.1. Objetivo General

- Crear una guía de implementación para el área de Seguridad de la Información basada en estándares internacionales.

2.2. Objetivos específicos

- Implementar en la guía las buenas prácticas establecidas por COBIT 5 e ITIL V3 2011.
- Integrar la guía de estándares de los procesos principales que se encuentran en la norma ISO 27002:2013 y el conjunto de debes de la 27001:2013.

3. Justificación

La presente investigación tiene como propósito la creación de una guía de implementación para el área de seguridad de la información basándose en las buenas prácticas y los estándares internacionales de las normas ISO, hemos propuesto la creación de la guía ya que al realizar una investigación sobre la seguridad de la información se ha observado mediante diferentes fuentes como US-CERT, ESET y ENISA (que son sitios que proporcionan estudios sobre la seguridad de la información) que cada vez los datos de una compañía se encuentran amenazados por diferentes tipos de vulnerabilidades y que con el paso del tiempo son más críticos, por lo que hemos sugerido esta guía con el fin de facilitar los pasos y consideraciones mínimas que una empresa debe cumplir, basados en los lineamientos establecidos en la norma ISO 27001:2013, ISO 27002:2013 y las buenas prácticas de COBIT 5.0, alineados con los objetivos de la organización y el área de tecnología de la información, y al mismo tiempo considerando algunos aspectos importantes sugeridos por ITIL V3 2011. Dicha guía, ayudará a aquellos miembros de una empresa que estén interesados en implementar el área de seguridad de la información, y tengan preguntas como: ¿qué debo considerar?, ¿por dónde inicio?, ¿cómo impactará a mi organización?, ¿qué lineamientos debería seguir para lograr tener un área de seguridad de la información con los objetivos, misión y visión correctos?, etc. De esta forma, se podrá minimizar el riesgo con el enfoque de esta área o el propósito para el cual está diseñada, así la organización también podrá ver este nuevo recurso como algo que genera valor a su compañía, cumpliendo el principal objetivo que es el de proteger la información sensible, minimizar riesgos y explotación de posibles amenazas que actualmente están afectando a la mayor parte de centro de datos, que no poseen las medidas necesarias para la seguridad de la información.

4. Alcances

- La investigación incluye únicamente la información de los siguientes documentos: ISO27001:2013, ISO27002:2013, COBIT 5 e ITIL v3 2011 apartado 4.7 Seguridad.
- La guía de implementación del área de TI está enfocada para toda empresa u organización que tenga la necesidad o el plan de apertura del área de Seguridad de la Información específicamente en un periodo finito de tiempo.

5. Limitantes

Meltdown y Spectre, las dos mayores fallas de seguridad anunciadas por los expertos en informática. De acuerdo con el área de investigación de Google, Project Zero, las fallas afectan a los microprocesadores en la mayoría de las computadoras del mundo, incluyendo dispositivos móviles y redes en la nube, y pueden permitir a los ciber delincuentes el acceso a la totalidad de los contenidos de la memoria de una computadora. (Fuente Eset Smart Security) de descubrir una vulnerabilidad, los ciberdelincuentes suelen preparar un exploit listo para usar. Luego pueden utilizar una técnica conocida como phishing como vector de infección para afectar usuarios y empresas a través de correos electrónicos con archivos adjuntos maliciosos. Incluso, tales vectores de ataques de suplantación de identidad son usualmente discretos y se usan muy activamente en ataques dirigidos más complejos. Tan solo en los últimos seis meses hubo muchos ejemplos de este tipo de evento.

Los ataques basados en esos exploits se consideran muy potentes, ya que no requieren interacciones adicionales con el usuario y pueden transmitir su código malicioso de forma discreta. Por lo tanto, son ampliamente utilizados, tanto por ciberdelincuentes que buscan ganancias como por medios más complejos respaldados por Estados con fines maliciosos, ver imagen 1 gráfico de ataques de exploits frecuentes.

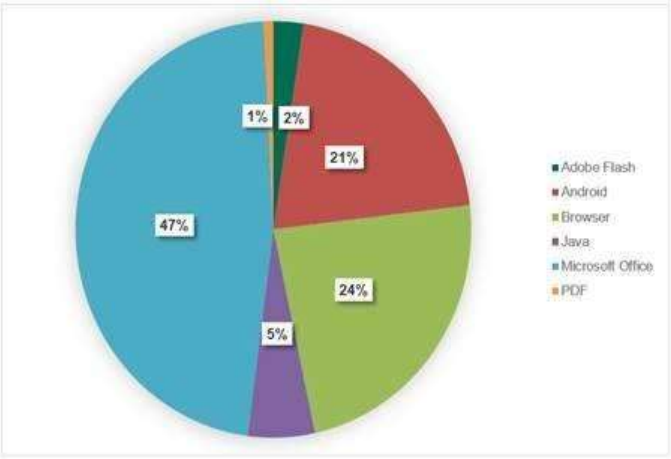

Imagen 1. Ataques basados en Exploits (Fuente Kaspersky)

6. Marco Teórico

6.1. COBIT 5

COBIT es publicado por el IT Governance Institute y por la Asociación de Control y Auditoría de Sistemas de Información (ISACA Information Systems Audit and Control Association). COBIT 5 es un marco de trabajo que permite comprender el gobierno y la gestión de las tecnologías de información (TI) de una organización, así como evaluar el estado en que se encuentran las TI en la empresa.

6.1.1. Principios de COBIT

COBIT se basa en 5 principios claves, para el gobierno y la gestión de las TI empresariales ver imagen 2.

Imagen 2. Principios de COBIT 5.

6.1.2. Procesos Habilitadores de COBIT 5

El modelo de referencia de Procesos de COBIT 5 subdivide las actividades y prácticas de la Organización relacionadas con las Tecnologías de la Información en dos áreas principales y 37 actividades (ver imagen 3):

1. Gobierno Corporativo de TI.

- Evaluar, Dirigir y monitorizar - 5 actividades de prefijo EDM.

2. Administración de TI Corporativa.

- Alinear, Planear y Organizar - 13 actividades de prefijo APO.
- Construir, Adquirir e Implementar - 10 actividades de prefijo BAI.
- Entregar, Servir y dar Soporte - 6 actividades de prefijo DSS.
- Monitorear, Evaluar y Valorar - 3 actividades de prefijo MEA.

Imagen 3. Modelo de referencia de procesos de COBIT 5.

De los procesos de COBIT 5 que se muestran en la imagen 3, se tomaron en cuenta 2 de los APOS para realizar la investigación y desarrollo de la guía y se describen a continuación en que consiste.

1. APO 12. Gestionar el Riesgo

- Este proceso consiste en identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
- Propósito del proceso es el de integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.
- Actividades
  - Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.

  - Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.

- Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.
- Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.
- Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.
- Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.
- Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.

2. APO 13. Gestionar la Seguridad
   - Descripción del proceso es el de definir, operar y supervisar un sistema para la gestión de la seguridad de la información.
   - Propósito del proceso es el de mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.
   - Actividades.
     - Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.
     - Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.
     - Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.
     - Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.
     - Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.
     - Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.
     - Comunicar el enfoque de SGSI.

6.2. ISO 27001:2013

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO), en esta norma se describe cómo gestionar la seguridad de la información en una empresa, su nombre completo es Tecnología de la información – Técnicas de seguridad – Sistema de gestión de seguridad de la información. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. La norma ISO 27001 puede ser utilizada e implementada por cualquier organización ya sea privada o pública, pequeña o grande. Esta proporciona una metodología para implementar la gestión dela seguridad de la información en una organización. Al mismo tiempo permite que una empresa sea certificada, es decir que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

La norma ISO 27001 se basa en la gestión de riesgos en la investigación de dónde se encuentran los riesgos y luego tratarlos sistemáticamente. Las medidas de seguridad que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero la utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales necesarias para prevenir violaciones de la seguridad.

ISO/IEC 27001:13 se divide en 11 secciones más el anexo A:

- Las secciones 0 a 3 son introductorias.
  1. Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
  2. Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.
  3. Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
  4. Sección 3 – Términos y definiciones – de nuevo, hacen referencia a la norma ISO/IEC 27000.

- Las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere

cumplir con la norma.

1. Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
2. Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
3. Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
4. Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
5. Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
6. Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
7. Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

- Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la declaración de aplicabilidad.
  1. Anexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones. (secciones A.5 a A.18).

6.3. ISO 27002:2013

En 2013, se publicó la versión actual. ISO 27002: 2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información, contiene 114 controles, a diferencia de los 133 documentados en la versión de 2005. Sin embargo, para la granularidad adicional, estos se presentan en catorce secciones, en lugar de los once originales.

El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la

seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa.

Finalmente, debe tenerse en cuenta que a lo largo de los años se han desarrollado o se están desarrollando varias versiones específicas de la industria de ISO 27002 (por ejemplo, sector de la salud, fabricación, etc.).

Las secciones de contenido de la ISO 27002:2013 son:

1. Estructura
2. Política de seguridad
3. Organización de seguridad de la información
4. Seguridad de recursos humanos
5. Gestión de activos
6. Control de acceso
7. Criptografía
8. Seguridad física y ambiental
9. Seguridad de las operaciones
10. Seguridad de Comunicaciones
11. Adquisición, desarrollo y mantenimiento de sistemas de información
12. Relaciones con proveedores
13. Gestión de incidentes de seguridad de la información
14. Aspectos de seguridad de la información de la continuidad del negocio
15. Conformidad.

6.4. ITIL V 3

ITIL (Information Technology Infraestructure Library o Biblioteca de Infraestructura de Tecnologías de la Información) es un compendio de publicaciones, o librería, que describen de manera sistemática un conjunto de "buenas prácticas" para la gestión de los servicios de Tecnología Informática (en adelante TI). ITIL no es un estándar que tiene que ser seguido; es una guía que debe leerse y entenderse, y utilizarlo para crear valor para el proveedor de servicios y sus clientes.

ITIL nació en la década de 1980, a través de la Agencia Central de Telecomunicaciones y Computación del Gobierno Británico (Central Computer and Telecomunications Agency - CCTA), que ideó y desarrollo una guía para que las oficinas del sector público británico fueran más eficientes en su trabajo y por tanto se redujeran los costes derivados de los recursos TI. Sin embargo, esta guía demostró ser útil para cualquier organización, pudiendo adaptarse según sus circunstancias y necesidades. De hecho, resultó ser tan útil que actualmente ITIL recoge la gestión de los servicios TI como uno de sus apartados, habiéndose ampliado el conjunto de "buenas prácticas" a gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones.

Estas buenas prácticas provienen de las mejores soluciones posibles que diversos expertos han puesto en marcha en sus organizaciones a la hora de entregar de servicios TI, por lo que en ocasiones el modelo puede carecer de coherencia.

En la actualidad ITIL pertenece al Oficina de Comercio Británico (Office of Government Commerce - OGC), pero puede ser utilizado para su aplicación libremente.

Ciclo de vida del servicio de ITIL.
La operación de servicio ITIL proporciona las mejores prácticas para la orientación de la etapa de operación del servicio del ciclo de vida del servicio ITIL ver imagen 4.

Imagen 4. Ciclo de vida del proceso ITIL.

ITIL tiene tres objetivos principales:

1. Mantener la satisfacción del negocio y la confianza en TI a través de una entrega efectiva y eficiente y soporte de servicios de TI acordados.
2. Minimizar el impacto de las interrupciones del servicio en el día a día actividades comerciales diarias.
3. Asegurar que el acceso a los servicios de TI acordados sea solo proporcionado a aquellos autorizados a recibir esos servicios. Y está confirmado por 9 secciones:

    1. Fundamentos de ITIL. Describe brevemente algunos conceptos básicos y la historia de ITIL, así como también sobre su utilidad.

    2. Estrategia del servicio. Este capítulo explica los conceptos de servicio administración y servicios, y describe cómo estos se pueden usar para crear valor. También resume una cantidad de conceptos genéricos de ITIL de lo que depende el resto de la documentación.

3. Diseño del servicio. Este capítulo describe algunas de los principios claves del funcionamiento del servicio que permitirán a los proveedores de servicios, planificar e implementar mejor las prácticas en la operación del servicio. Estos principios son independientes de la organización; sin embargo, el enfoque puede necesitar ser adaptado a las circunstancias, incluido el tamaño de organización, distribución geográfica, cultura y recursos disponibles. El capítulo concluye con las principales entradas y salidas para la etapa del ciclo de vida de la operación del servicio.
4. Transición del servicio. Establece los procesos y actividades de las que depende la operación efectiva del servicio y cómo se integran con las otras etapas del ciclo de vida.

5. Operación del servicio. Identifica las actividades operacionales requeridas para administrar de forma efectiva y eficiente los servicios en el día a día para ofrecer valor al negocio. Aborda muchos de los puntos comunes y actividades operacionales que las organizaciones utilizan para operar sus servicios tales como la programación de trabajos, copia de seguridad y restauración, la administración de servidores, red y escritorio.

6. Mejora continua del servicio. Este capítulo identifica los roles organizacionales y responsabilidades que deberían ser consideradas para administrar la etapa del ciclo de vida de la operación del servicio y sus procesos asociados. Estos roles son proporcionados como pautas y se puede combinar para encajar en una variedad de estructuras organizacionales.

7. Consideraciones tecnológicas. Este capítulo proporciona recomendaciones para el uso de la tecnología en la operación de servicio y los requisitos básicos que un proveedor de servicios deberá considerar cuándo elija herramientas de gestión de servicios.

8. Implementación de la operación del servicio. Para organizaciones nuevas en ITIL, o aquellos que desean para mejorar su madurez y capacidad de servicio, este capítulo describe formas efectivas de implementar la etapa del ciclo de vida de la operación del servicio.

9. Desafíos, riesgos y factores críticos del éxito. Es importante para cualquier organización comprenda los desafíos, riesgos y factores críticos de éxito que podrían influir en el éxito de su implementación. Este capítulo analiza ejemplos típicos de estos, para diferentes escenarios del ciclo de vida de la operación del servicio.

6.5. Seguridad de la información

La Gestión de la Seguridad de la información, al igual que otros elementos de gestión de las buenas prácticas de ITIL, implica gestionar correctamente las implicaciones que se deriven de la puesta en marcha de un servicio IT en ámbitos de seguridad, de manera que este servicio no sea (en este caso) disminuido, atacado o colapsado por elementos que interfieran en los flujos correctos de información.
La información es la fuente principal en muchos casos de los éxitos o fracasos de las organizaciones. Ésta además se interrelaciona totalmente con ITIL y su modelo de Gestión, ya que la información posee tres pilares o propiedades que la hacen susceptible de ser un aspecto que cuidar; las mismas a las que se refiere la ISO 27001, que son: la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para una compañía;

- Confidencialidad: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
- Integridad: es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
- Disponibilidad: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

La información sean electrónicos, en papel, audio o video de una entidad son bienes importantes por lo que se requiere que sean protegidos con políticas, procesos y procedimientos que ayuden a salvaguardar los datos ante amenazas que atenten contra la disponibilidad de está. Por lo que es recomendable diseñar un sistema de gestión de seguridad de la información SGSI.
La norma ISO 27001 presenta los requisitos básicos para implementar un SGSI, según la norma el objetivo de un SGSI es el de la protección de la información y los sistemas de información de acceso, de utilización, divulgación o destrucción no autorizada. Para ello se debe de contar con un estándar que plantee un SGSI y que enfatice la importancia de:

1. Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
2. Implementar y operar controles para manejar los riesgos de la seguridad de la información.
3. Monitorear y revisar el desempeño y la efectividad del SGSI.
4. Mejoramiento continuo en base a la medición del objetivo.

Este estándar debe de adoptar un modelo de proceso que ayude a la planificación y al mejoramiento continuo para obtener los resultados que se esperan al implementar un área de Seguridad de la información dentro de la organización, por lo que se promueve la adopción del modelo PDCA aplicados

a los procesos SGSI, ver imagen 5 para ver ejemplo del modelo, al mismo tiempo se aclara que existen otros tipos de métodos que pueden aplicarse en el proceso de la mejora continua del SGSI lo que dependerá de la entidad la que desee adoptar.

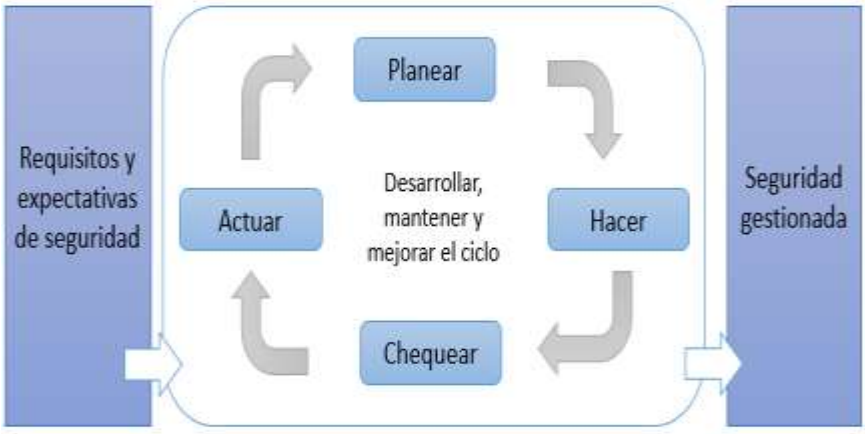

Imagen 5. Modelo de PDCA aplicado a los procesos de SGSI.

La imagen anterior demuestra como es el proceso del ciclo para la mejora continua de los procesos del SGSI, dentro de los cuales se identifican procesos claves como lo es planear, hacer, chequear y actuar. En la tabla N° 1 se puede identificar la función de cada proceso clave dentro del modelo PDCA.

Planear (Establecer el SGSI)	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad que sean necesarios para la gestión del riesgo y mejoramiento de la seguridad, con el fin de entregar resultados relacionados con las políticas y objetivos de la organización.
Hacer (Implementar y operar el SGSI)	Garantizar que la implementación de los controles, procedimientos y procesos, sean aplicados de una manera correcta y adecuadamente.
Chequear (Revisar y dar seguimiento)	Evaluar que la aplicación de los procesos y controles creados, se encuentren desempeñándose acordes a la política y objetivos de seguridad.
Actuar(Mantener y mejorar el SGSI)	Realizar acciones correctivas y preventivas que se basen en los resultados o auditorías de la verificación y revisión de los controles, políticas, procesos y procedimientos para la mejora continua del SGSI.

Tabla N° 1. Descripción de los procesos del modelo PDCA.

Dentro del estudio de las normas ISO 27001:2015, 27002:2015, COBIT e ITIL, se encontraron procesos claves con los que conformamos la imagen 6 donde se demuestra un modelo de procesos del ciclo que posee un Sistema de Gestión de Seguridad de la Información, es como se ha identificado las diferentes gestiones que conforman al SGSI y los procesos estratégicos, operativos o de apoyo.

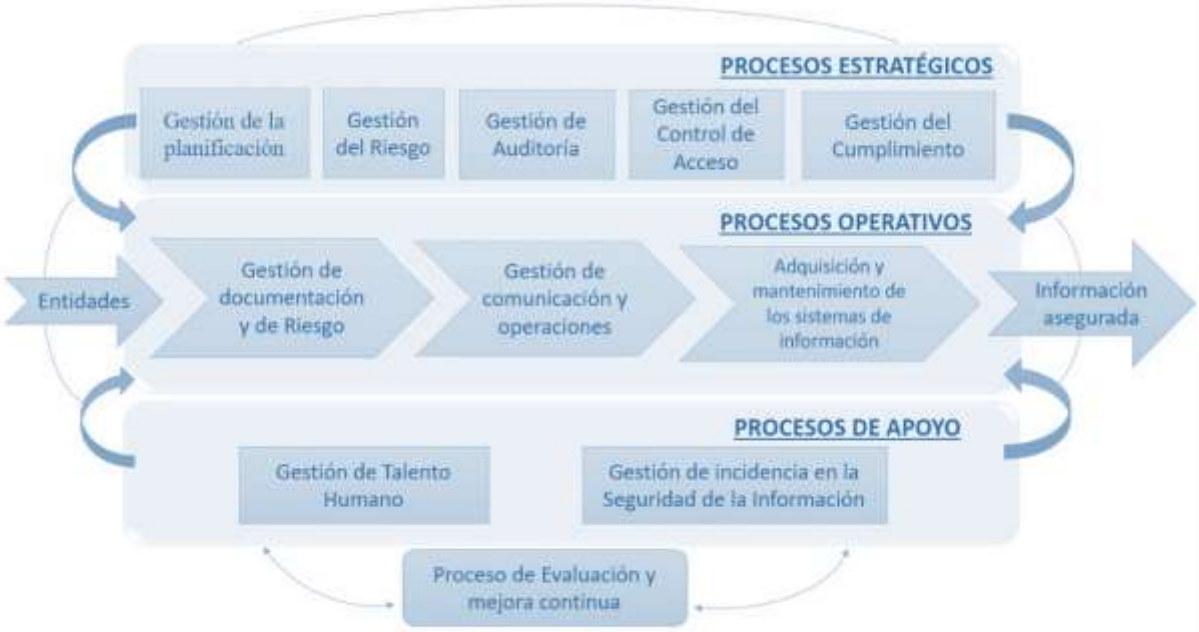

Imagen 6. Mapa de procesos de un SGSI.

ITIL recomienda realizar un seguimiento muy ligado a los objetivos y protocolos, el seguimiento trabaja a través de indicadores de rendimiento que aportan información sobre cómo se están ejecutando los protocolos de actuación, las mejoras derivadas del análisis de estos y si se están logrando los objetivos propuestos. Y Mejora de Seguridad, en cuanto a las auditorías de seguridad son elementos clave para la mejora continua y el seguimiento de la gestión de la seguridad ya que aseguran, por parte de agentes muy cualificados, internos o externos, si la seguridad está siendo la correcta y en qué aspectos se puede mejorar.

7. Guía de implementación del área de seguridad de la información como un servicio de TI basado en las buenas prácticas de COBIT 5, ISO 27001:2013 e ITIL v3 2011.

A lo largo del desarrollo que se describe a continuación, se realiza un marco que se encuentra relacionado con la norma ISO 27001, COBIT e ITIL, por lo se demuestra la integración de un todo de estos estándares y buenas prácticas en la imagen 7.

Imagen 7. Componentes de estándares y buenas prácticas.

7.1. Evaluación y control de riesgos

De acuerdo con ITIL, apartado 3.4 la Gestión de la Seguridad de la información, al igual que otros elementos de gestión de las buenas prácticas de ITIL, implica gestionar correctamente las implicaciones que se deriven de la puesta en marcha de un servicio IT en ámbitos de seguridad, de manera que este servicio no sea (en este caso) mermado, atacado o colapsado por elementos que interfieran en los flujos correctos de información.

La Gestión de la Seguridad está íntimamente relacionada con multitud de procesos, y por tanto requiere de una coordinación correcta con toda la organización que gestione la infraestructura y el servicio. Así se establecen unos documentos y protocolos de actuación desarrollados en los puntos siguientes:

1. Debe existir una Política de Seguridad que sirva de guía y ejemplo a la organización.
2. De esta Política deben derivar unos objetivos que se han de ver plasmados en un Plan de Seguridad que incluirá los niveles de seguridad acordados con el cliente se según sus necesidades en los SLAs y con los proveedores, a través de los UCs.

3. Este Plan de Seguridad debe ser puesto en marcha y seguido, así como evaluado.
4. El Plan de Seguridad debe disponer de un listado (base de datos) donde se detallen los elementos a seguir (activos) y sus vulnerabilidades, así como los riesgos reales y potenciales.

Para ello es recomendable realizar la evaluación de riesgos informáticos, que involucra la identificación de activos informáticos con sus respectivas vulnerabilidades y amenazas a los que se encuentran expuestos a así evaluar la probabilidad de ocurrencia y el impacto que éstos generarían, todo esto con el objetivo de determinar, los controles adecuados para estimar, aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. Para dicha evaluación, como mínimo se recomienda realizar los siguientes puntos:

7.1.1. Identificación de riesgos, estudiar cuidadosamente los posibles riesgos que se puedan materializar o explotar considerando el impacto que ello podría causar.

7.1.2. Análisis de riesgos, involucra la estimación del impacto que tendrán los riesgos identificados, dentro de una organización. Para el análisis de riesgos se podrían considerar las siguientes preguntas por cada uno identificado y así poder tener una mejor visibilidad del impacto que éste podría causar:

- ¿Qué podría fallar?
- ¿Con qué frecuencia se podría presentar u ocurrir?
- ¿Qué consecuencias se tendrían?
- ¿Cuán fiables son las respuestas a las primeras tres preguntas?
- ¿Durante cuánto tiempo podría estar la organización abierta y sin sistemas?
- ¿Cuánto sería el costo para la compañía por estar sin operación durante minutos, horas, días o semanas?
- ¿Cuánto tiempo podría estar la organización fuera de línea sin que sus clientes se vayan con la competencia?
- ¿Se tiene forma de identificar personas deshonestas o con intenciones maliciosas en el sistema?
- ¿Hay controles sobre la operación de cada sistema?
- ¿Qué se considera, dentro de la organización como información sensible o confidencial?
- ¿Cómo se almacena la información sensible en los sistemas?
- ¿Se tiene medidas de seguridad actualmente que cubra diferentes tipos de ataques tecnológicos?
- ¿Existen controles de acceso?
- ¿Qué acciones se tomarían si la seguridad fuera violada?

7.1.3. Evaluación de riesgos, una vez identificados y analizados los riesgos, es importante identificar el nivel de riesgo que tendría, ejemplo:

Activos	Tasación				Amenazas	Posibilidad ocurrencia	Vulnerabilidad	Posible explotación de vulnera-bilidad	Valor activo	Posible ocurrencia	Total
	Confiden-cialidad	Integri-dad	Disponi-bilidad	Total							
1) Datos del cliente	A	A	A	A	- Plagio - Falsificación - Alteración - Privacidad	B B B A	- Deficiencia org. - Deficiencia envio - Acceso no autorizado - Control documentos	B A A M	A	M	M
2) Factura como documento	A	A	A	A	- Pérdida documento - Retraso en entrega - Ilegibilidad de datos - Cargos incorrectos	A A B M	- Datos incompletos - Desconocimiento rutas - Deficiencia impresión - Errores de procesamiento	A A B A	A	M	M
3) Tarifas	A	A	A	A	- Alteración incorrecta - Ignorancia cambios - Ofertas	B M A	- Acceso no autorizado - Mal entrenamiento - Falta comunicación	M B M	A	B	B
4) Servicios brindados	B	A	A	A	- Mala interpretación - Poco detalle - Servicio no solicitado	M A M	- Personal no calificado - Reducción costo - Error digitación	M A M	A	M	M
5) Software de facturación	A	A	A	A	- Errores de código - Códigos maliciosos - Fallos técnicos - Errores usuario - Falta seguridad	M A M B A	- Personal no calificado - Controles acceso - Energía eléctrica - Mal entrenamiento - Falta políticas	B M A B A	A	A	A
6) Medio de comunicación y/o entrega	A	A	A	A	- Fallas funciona-miento - Falta seguridad - Falta personal	A A B	- Energía eléctrica - Errores configuración - Poca disponibilidad	A M B	A	A	A

Tabla N°2 Análisis y evaluación del riesgo.

A: Alto B: Bajo M: Medio

En la tabla N° 2, se muestra el resultado final de la identificación y análisis del riesgo. Para iniciar, es necesario realizar la identificación de los activos de información sensibles, vitales y confidenciales. Luego se procede a identificar la protección apropiada para cada activo identificado, para ello es necesario determinar su valor en términos comerciales o en ciertos casos determinar su valor potencial y el impacto en relación con su confidencialidad, integridad y disponibilidad. Para ello se puede clasificar entre las escalas que se considere conveniente, para el ejemplo, se clasificaron entre ALTO, MEDIO o BAJO.

Una vez realizada la evaluación de valor e impacto, se procede a identificar las posibles amenazas que tengan la capacidad de causar incidentes no deseables, que causen daños a la organización, sistemas o sus activos, para ello se podrían reunir personas de las diferentes áreas involucradas para realizar lluvia de ideas sobre los activos que estén relacionados.

La posibilidad de ocurrencia de las Amenazas puede ser variable para cada activo, ya que no todas pueden tener la misma probabilidad de ocurrencia. En este caso, es recomendable que un equipo con experiencia y conocimiento sobre los activos y las amenazas evalúe la posibilidad de ocurrencia de cada uno.

Las vulnerabilidades son debilidades que están asociadas a cada activo y que pueden permitir que las amenazas las exploten y causen daños, por lo tanto, un equipo conformado por personas con experiencia y conocimiento de las diferentes vulnerabilidades, podrían identificar las posibles explotaciones de vulnerabilidades y luego evaluar la posible explotación por cada amenaza.

El siguiente paso sería evaluar los riesgos contemplando dos factores básicos: Estimar el valor de los Activos en Riesgo para determinar el daño económico que el riesgo podría causar a los activos de información y la posibilidad de Ocurrencia del Riesgo estudiando por cada activo sus impactos, amenazas y posibilidad de ocurrencia, así como también las vulnerabilidades y su posibilidad de ser explotadas.

Finalmente, establecer el Valor del Riesgo de los Activos para establecer sus respectivos controles.

7.1.4. Examinar y evaluar la gestión de riesgos.

De acuerdo con la norma ISO 27001:2013 esta hace más énfasis en medir y evaluar, sin embargo, Cobit5, dentro de la práctica de gobierno del APO12 EDM03.01 examina y evalúa la gestión de riesgos, ITIL V3:2011 literal 9.3 habla de los proyectos planificados ayudarán a identificar riesgos de implementación.

Estos riesgos pueden incluir:

1. Cambio en las responsabilidades en proyectos existentes que desmotivan la fuerza de trabajo
2. Costos adicionales no planificados a los servicios.
3. Falta de madurez e integración de sistemas.
4. Resistencia al cambio y elusión de procesos debido a la burocracia percibida.
5. Entre otros.

Verificar y vigilar tanto el monitoreo como la actualización del proceso para la gestión del riesgo. Dicha actualización puede ser realizada mediante reuniones anuales donde se evalúen los riesgos o si es necesario se realice a raíz de un riesgo que para la compañía sea alto o grave y no esté registrado. Para ello, la dirección tiene la responsabilidad de examinar y revisar de acuerdo con la periodicidad que sean definidas internamente.

Los procesos de monitoreo y revisiones deben considerar todos los aspectos del proceso para la gestión del riesgo con el objetivo de:

1. Garantizar que los controles definidos son eficaces y eficientes tanto en diseño como en la operación.

2. Obtener información adicional para mejorar la valoración del riesgo.
3. Analizar y aprender lecciones a partir de los eventos (incluyendo los accidentes), los cambios, las tendencias, los éxitos y los fracasos.
4. Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios del riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades.

5. Identificar los riesgos emergentes. El avance en la implementación de los planes para tratamiento del riesgo suministra una medida de desempeño. Los resultados se pueden incorporar en las actividades globales de gestión del desempeño, medición y reporte externo e interno de la organización.

7.1.5. Aplicación y evaluación de riesgos.

Para la Aplicación y Evaluación de riesgos comprende la identificación de los riesgos asociados con la operación de la compañía y su evaluación; así como también identificar riesgos en planes de trabajo y evaluar los riesgos que están asociados con las incidencias y la gestión de cambio.

También se puede asociar las evaluaciones del riesgo con clasificaciones específicas. Especificar los atributos de una clasificación para cada evaluación del riesgo con la que los desee utilizar, y definir formatos estandarizados para llevar a cabo las evaluaciones del riesgo. Puede utilizar las mismas clasificaciones para evaluaciones del riesgo de diferentes áreas de la organización para mejorar la coherencia del proceso de evaluación del riesgo.

La matriz de riesgos, que se define en la aplicación Matriz de riesgos, se utiliza para asignar las clasificaciones de riesgo al trabajo.

7.1.6. Selección de técnicas para la evaluación de riesgos

Existen diversidad de técnicas para la evaluación de riesgos, cada organización puede seleccionar la que considere conveniente, a continuación, se presenta una breve lista entre las que se puede elegir:

a. **Brainstorming o Tormenta de ideas:** No es un método específico para la identificación de riesgos, pero se utiliza habitualmente en departamentos relacionados con creación y el diseño de productos. Sin embargo, también se puede aplicar a este ámbito. Dejar espacio a la imaginación, diversos puntos de vista, a la creatividad y al intercambio de ideas puede permitir descubrir riesgos no identificados y de esa manera tomar las medidas pertinentes ante ellos.

b. **Checklists o Listas de comprobación:** Consisten en listas de signos de alarma o puntos de control que se deben comprobar para asegurar que no se produce ningún error significativo en la ejecución del proyecto (ver Anexo 1 ejemplo de checklist). Una

ventaja fundamental es su sencillez, aplicabilidad a múltiples tareas y proyectos y que, si se han elaborado adecuadamente, evitan que se cometan errores graves. Sin embargo, depositar excesiva confianza en estas listas puede conducir a instaurarse en la comodidad de evitar hacer un análisis exhaustivo de los riesgos de cada tarea.

c. **SWIFT (Structured What If Technique):** Prácticamente consiste en, plantear las consecuencias que determinados acontecimientos podrían tener para la organización. SWIFT es muy útil para recopilar una serie de riesgos, que se estructuran en una secuencia lógica. A continuación, se analizan en detalle atendiendo a sus posibles causas y consecuencias, lo que permite identificar interdependencias para, acto seguido, plantear planes de respuesta.

d. **Fault Tree Analysis o Análisis de fallos en forma de árbol:** Es una técnica útil para identificar y analizar las causas que conducen a un evento no deseado. Éste se coloca en la parte superior del esquema y posteriormente se dibujan líneas en forma de árbol invertido, identificando en sucesivos niveles las causas que han conducido hasta él. En una reunión en la que se utilice este tipo de análisis, se argumentan posibles causas que producen un determinado evento. Depende de los niveles en los que se desarrolla el árbol, se pueden incluir causas de las primeras causas, con lo que se profundiza todavía más en la raíz del problema. Dado el énfasis de esta técnica en la causalidad, adquiere especial importancia en la búsqueda de soluciones. Una vez identificada la causa original del problema, se deben buscar métodos para mitigar y así proponer solución a todas las consecuencias derivadas.
e. **Análisis de Montecarlo:** Es un sistema de análisis matemático complejo mediante el cual se realizan aproximaciones aritméticas para cálculos de los cuales no se puede obtener una solución exacta. Mediante programas informáticos especializados se simulan diferentes riesgos a los que se considera sucesos aleatorios, teniendo en cuenta el impacto que cada uno supondría para cada activo y la probabilidad de que se presenten.

7.2. Políticas de seguridad de la información

De acuerdo con la ISO 27002:2013, el objetivo de las políticas de seguridad de la información es proporcionar directrices y apoyo para la seguridad de la información en concordancia con los requerimientos del negocio, leyes y regulaciones pertinentes.

La norma recomienda establecer un conjunto de políticas de seguridad de la información, el cual debe ser definido y aprobado por la Dirección, publicado y comunicado a todos los empleados y entidades externas relacionadas. Dichas políticas deben ser revisadas periódicamente, según la organización lo planifique o siempre que se produzcan cambios significativos para asegurar que se mantenga su continuidad, idoneidad, adecuación y efectividad.

Las políticas de seguridad de la información deben considerar los requerimientos creados por:

a. La estrategia de negocios de la organización, esto puede ser apartados de la política vigente del área;
b. Reglamentos, legislaciones y contratos relevantes que se consideren de alto nivel, confidenciales y sensibles;
c. Amenazas ambientales actuales y proyectadas a la seguridad de la información, considerar los planes de acción ante la ocurrencia de una amenaza ambiental, según aplique para el radio periférico de la organización a nivel físico como digital.

Como parte de la política de la seguridad de la información debe considerar declaraciones relativas a:

a. Definición de seguridad de la información, objetivos y principios para guiar todas las actividades relativas a la seguridad de la información;
b. Asignación de responsabilidades generales y específicas para la gestión de seguridad de la información a roles definidos;
c. Procesos de manejo de las desviaciones y excepciones.

7.3. Gestión de activos

La gestión de activos comprende identificar los activos de la organización y definir los planes de protección con sus respectivos responsables de ejecución.

Para realizar la gestión de activos, la ISO 27002:2013 sugiere realizar el control de la información, en el que otros activos asociados con información e instalaciones de procesamiento de la información deben ser identificados en un inventario que estén siendo actualizado constantemente. El inventario de activos debe ser exacto, actualizado, consistente y alineado con otros inventarios.

Cada inventario realizado, debe ser asignado mediante un proceso, para garantizar la asignación oportuna de propiedad de los activos. La propiedad debe ser asignada cuando se crean los activos o cuando los activos se transfieren a la organización. El propietario de los activos debe ser responsable de la correcta gestión de un activo durante todo el ciclo de vida de los activos.

Todos los empleados y usuarios externos deben devolver los activos de la organización que se encuentren en su posesión una vez dada la terminación de su empleo, contrato o acuerdo, por lo que es recomendable que se defina un proceso de terminación formalizado, para incluir la devolución de todos los activos físicos y electrónicos emitidos, asignados o encomendados por la organización.

7.4. Control de acceso

El control de acceso en una organización es donde se pueden conocer los ingresos a un lugar físico o sistema de un usuario en particular, mediante el almacenamiento de esta información en controles de bitácoras de accesos.

Para la creación e implementación de un control de acceso se debe de tener en cuenta los siguientes criterios mínimos:

1. Se debe poseer un requerimiento del negocio para la creación de un control de acceso.
2. Se debe de poseer una política del control de acceso en base a las necesidades del negocio y requerimientos de creación.
3. Se debe establecer, documentar y revisar la política de control de acceso basada en los requerimientos de seguridad de la información y del negocio
4. Se debe de Poseer una bitácora de control de acceso vigente autorizada y capacitar a los usuarios responsables de estas.

7.5. Criptografía

Según la UNAM de México, criptografía proviene del griego kryptos: "ocultar", y grafos: "escribir". Es decir, significa "escritura oculta". Como concepto son las técnicas utilizadas para cifrar y descifrar información utilizando técnicas matemáticas que hacen posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Poseer una política que asegure el apropiado uso de la criptografía ayuda a proteger la confidencialidad, autenticidad e integridad de la información que se mantiene almacenada en los diferentes sistemas o espacios físicos dentro de una organización.

Para ello es necesario que se cuente con controles de cifrado como los siguientes.

1. Controles criptográficos en los que ayuden a mantener la seguridad de datos confidencialmente.
2. Evaluación del riesgo, fortaleza y calidad del algoritmo de cifrado que se requiere para asegurar la confidencialidad.
3. Creación de Roles y responsabilidades que ayuden a controlar la seguridad criptográfica que contiene cada proceso.

4. Generación de llaves y gestión de control.

Mediante la creación de política para el uso protección y duración de las llaves criptográficas podemos proporcionar seguridad a nuestra información, para ello se deben especificar los controles necesarios para la vida de una llave (ver Sección 10.1.2 de la norma ISO 27002:2013):

1. Determinar los requisitos y el ciclo de vida de una llave criptográfica.
2. Proporcionar protección de su almacenamiento y alteración o pérdida del uso de las llaves.
3. Protección del uso inadecuado y no autorizado.
4. Creación de un sistema de gestión de llaves con sus normas, procedimientos y métodos seguros.
5. Registrar y auditar las actividades de gestión relacionadas con las llaves.
6. Normas que se apliquen en la organización.
7. Considerar las regulaciones y restricciones nacionales que apliquen en las técnicas de criptografía.
8. Creación de controles criptográficos.
9. Identificación de maximizar los beneficios y minimización de riesgos.

7.6. Estructura de la Seguridad

7.6.1. Seguridad física y ambiental

La seguridad física ayuda a mantener identificado el perímetro donde se encuentran ubicados los centros de datos y puntos de distribución de los diferentes accesos de red que necesiten mantenerse en áreas seguras protegidas por las reglas o controles de seguridad definidos, barreras de seguridad o controles de acceso no autorizados, daño e interferencia.

Se debe de identificar las áreas seguras determinando lo siguiente:

1. Se debe identificar el perímetro de seguridad física y ambiental.
2. Se debe de crear una política del control de seguridad física y ambiental.
3. Se debe definir los controles de las áreas y perímetros de seguridad para su protección.
4. Se debe de identificar el perímetro físico y ambiental que sean accesos directos a áreas restringidas, así también determinar si se encuentran en buenas condiciones físicas y posea mecanismos de control de acceso.
5. Se deben de poseer controles de entrada físicos.
6. Se debe determinar un diseño que sea aplicado para evitar amenazas de catástrofes naturales o ataques provocados por el ser humano.
7. Se debe de crear y diseñar procedimientos para trabajar en áreas seguras tanto para los empleados como usuarios externos.
8. Se debe crear controles de puntos de accesos de carga y descarga, evitando que sea un acceso no autorizado para personas que no tienen permiso de ingresar a zonas o áreas seguras no autorizadas.

9. Se deben crear controles de ubicación y protección del equipo ante amenazas y peligros ambientales como temperaturas muy altas o bajas y humedad, protección contra rayos se debe de proteger las líneas de comunicación y energía
10. Se deben crear controles que ayuden a proteger los equipos por cualquier falla en las herramientas de soporte y que estas cumplan con las especificaciones del fabricante del equipo y los requisitos legales locales, como también incluir los tipos de mantenimientos que deben de realizarse para asegurar la disponibilidad de estos.
11. Se debe de crear controles que protejan el cableado ante intercepción, interferencia o daño.
12. Se debe determinar el personal de mantenimiento que se encontrará autorizado de realizar estas gestiones, así como también llevar el registro de todos los fallos sospechosos o reales y de todo el mantenimiento preventivo y correctivo.
13. Crear controles y procedimientos que determinen las medidas de seguridad que se deben de considerar antes diferentes riesgos que implica que un equipo o activo se encuentra fuera de las instalaciones.
14. Se debe crear el procedimiento donde indique los pasos a seguir para eliminar o sobrescribir la información de datos y software antes de su reutilización o eliminación
15. Se debe crear procedimientos que ayuden a mantener la seguridad en los equipos que se encuentran activos sin un bloqueo de pantalla con alguna contraseña.
16. Se debe desarrollar una política donde se especifique las acciones que se deben de tomar en cuenta para mantener el área de escritorio limpio para documentos y medios de almacenamiento, y también en las instalaciones de procesamiento de la información

7.6.2. Seguridad de las operaciones

La seguridad de las operaciones consiste en verificar que las operaciones sean correctas y seguras desde donde se procesa la información, por medio de esto se demuestra la confiabilidad de sus datos y credibilidad de quienes tienen acceso a esta información.

Se deben de tomar los siguientes criterios para crear procedimientos en donde se logre la seguridad de las operaciones:

1. Se debe de poseer una política de la seguridad de las operaciones de acuerdo con el negocio.
2. Se debe contar con un manual de procedimientos y responsabilidades operacionales.
3. Se debe poseer procedimientos de operación de documentos en donde se especifique las instrucciones que deben de tomarse ante las actividades que se encuentran asociadas a los sistemas como: instalación y procesamiento de información, respaldo, mantenimiento, manejo de medios y que deben estar al alcance de todos.

4. Se debe de poseer un control donde se especifique la manera de actuar para los cambios que se dan constantemente en la organización, procesos de negocios, instalaciones de procesamiento de la información.
5. Se debe mantener un control de los recursos que se encuentran en uso, su utilidad, y también verificar la optimización y desempeño de estos.
6. Se debe de tener un control en donde se identifique la separación de los ambientes de producción, contingencia, pruebas y desarrollo, para reducir los riesgos de accesos no autorizados o cambios en el ambiente de producción, así como definir los procedimientos y reglas para transferir actualizaciones, cambios o mejoras de desarrollo a producción, deben de funcionar en sistemas diferentes y dominios o directores distintos.
7. Se debe de poseer un control para la realización de pruebas en un ambiente que no sea el de producción.
8. Se deben de crear controles contra software malicioso donde los detecte, prevea y recupere
9. Se debe de poseer controles en caso de contingencia para la continuidad de negocio apropiado para la recuperación ante los ataques de software malicioso, problemas con equipos y otros.
10. Se debe crear una política con sus controles y procedimientos para el respaldo de sistemas, imágenes del sistema, base de datos e información sensible para el negocio, en donde se especifique la periodicidad de las actividades de copias de seguridad de la información y pruebas periódicas de funcionamiento.
11. Se debe de elaborar un control donde se especifiquen las medidas que se deben de tener al momento de monitorear o revisar los logs de los diferentes archivos de sistemas, fallas, excepciones, actividades del usuario y eventos de seguridad de la información.
12. Se debe crear un control donde se lleve un historial de instalaciones de equipos con su bitácora.
13. Se debe de contar con controles de bitácoras de auditoría en donde se especifiquen las observaciones.
14. Se debe de contar con un control donde se almacene las actividades del administrador y operador del sistema, además de ser protegidas y revisadas regularmente.
15. Se debe de contar con un control donde se especifique la sincronización del reloj en de los diferentes servidores que se posean.
16. Se debe de contar con procedimientos para controlar la instalación de software en los sistemas operacionales.

17. Se debe de crear un control donde se especifique el procedimiento para obtener las vulnerabilidades los sistemas de información usados, así como evaluar los riesgos que sean considerados a la organización y previniendo con las medidas apropiadas para abordar el riesgo asociado.
18. Restricciones en la instalación de software. Creación de controles con procedimientos donde se especifique los procesos para la instalación de software por parte de los usuarios
19. Consideraciones en la auditoría de sistemas de información
20. Controles de auditoría de los sistemas de información
21. Crear un control donde se identifique los requerimientos y actividades de auditoría que involucran los sistemas en producción deben ser cuidadosamente planificados y acordados para minimizar las interrupciones a los procesos de negocio.

7.6.3. Seguridad de las comunicaciones

La seguridad de comunicaciones debe de poseer procedimientos que ayuden a delimitar mediante políticas la gestión de la seguridad de la información en redes y su soporte a las instalaciones de procesamiento de información.

Para crear los controles de seguridad de la red se debe de tener en cuenta lo siguiente:

1. Se debe crear un control que gestione procedimientos para proteger las redes y la información en los sistemas, para salvaguardar la información que se procesa se deben establecerse responsabilidades y procedimientos para la gestión de los equipos de redes.
2. Se debe de crear un control donde se posea la gestión de todos los servicios de red, deben ser identificados e incluidos en cualquier acuerdo de servicios de red, ya sea si estos son provistos por la misma organización o se subcontratan.
3. Se debe de crear un control donde se segmenta en redes los grupos de servicios de información, usuarios y sistemas de información.
4. Se deben de crear procedimientos y políticas de transferencia de información, además de controles formales para proteger la transferencia de información a través del uso de todos los tipos de medios de comunicación.
5. Se deben de crear controles donde se especifiquen los diferentes acuerdos para lograr la seguridad de la transferencia de información del negocio entre la organización y entidades externas.
6. Se debe de crear controles donde se especifique la protección adecuada de la diferente información contenida en los mensajes electrónicos
7. Se deben identificar, revisar periódicamente y documentar los requerimientos para acuerdos de confidencialidad, reflejando las necesidades de la organización para la protección de la información.

7.7. Adquisición desarrollo y mantenimiento de los sistemas

7.7.1 Relación con proveedores.

Todo el personal externo que desarrolle labores en la empresa deberá cumplir con la política de seguridad recogida en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones se reserva el derecho de veto sobre el personal externo que haya cometido la infracción, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación con la empresa contratada.

El principal objetivo del presente documento es mitigar los riesgos asociados a los sistemas de información describiendo lo que se espera de todo el personal que pertenece a otras empresas proveedoras que trabajan para que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas.

Asimismo, se pretende fomentar el uso de buenas prácticas en materia de seguridad de la información para ello, las empresas proveedoras a las que se les remita este documento se responsabilizan de informar de las normas incluidas en el mismo a las personas que destinen a prestar sus servicios.

Esta política de Seguridad refleja requerimientos legales y éticos aplicables sobre:

1. Proteger la información confidencial perteneciente o cedida por terceros a de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
2. Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
3. Obtención de acceso a los sistemas de información propios o bajo supervisión será necesario disponer de un acceso autorizado.
4. El personal externo que tiene acceso a información debe considerar que dicha información, por defecto, tiene el carácter de confidencial. Se puede considerar como información no confidencial aquella información a la que haya tenido acceso a través de los medios de difusión pública de información.
5. Los usuarios protegerán la información confidencial a la que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información.
6. Conocer, aceptar y cumplir la presente Política antes de poder acceder a los sistemas de información. De forma adicional, todo el personal con responsabilidades específicas dentro del ámbito de actuación indicado debe asegurarse de que se cumplen las siguientes medidas:

a. Con carácter general, todo diseño, desarrollo, implementación y operación deberá incorporar mecanismos de identificación, autenticación, control de acceso, auditoría e integridad, que se especificarán para cada caso concreto.
b. Incorporar identificaciones seguras y únicas para la autenticación de usuarios.
c. Para un correcto funcionamiento en materia de seguridad deben compartirse las labores de seguridad entre usuarios, administradores y los encargados directos de la propia seguridad.
d. Tomar todas las precauciones posibles para proteger físicamente los sistemas y prevenirlos frente al robo, destrucción o interrupción.
e. Definir un plan de recuperación del sistema para el caso en que se dé robo, destrucción o interrupción del servicio.
f. Asegurar la confidencialidad de la información almacenada, tanto en formato electrónico como no electrónico.
g. Todos los intervinientes en el plan de continuidad de negocio deben conocer y saber aplicar cuando sea necesario dicho plan.
h. El personal del área de operación deben tener conocimiento de los procedimientos de recuperación de datos de carácter personal, de los soportes de datos de carácter personal y del procedimiento de registro entrada/salida de dichos soportes.

7.7.2 **Confidencialidad de la Información**.

La confidencialidad de la información se define como la garantía de que la información no es divulgada de forma inadecuada a entidades o procesos.

1. El personal externo que tenga acceso a información deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información a la que haya tenido acceso a través de los medios de difusión pública de información.
2. Los usuarios protegerán la información confidencial a la que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información.
3. Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior información confidencial en cualquier tipo de soporte, salvo que esté debidamente autorizado.

4. Se utilizará el menor número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
5. En relación con la utilización de agendas de contactos dispuestas (por ejemplo: Outlook) el personal externo únicamente introducirá determinados datos personales que sean indispensables como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
6. Ningún colaborador externo en proyectos o trabajos puntuales deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada tanto ahora como en el futuro.
7. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
8. Asimismo, el empleado de la empresa proveedora deberá devolver el o los soportes mencionados inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación de su empresa. La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y sin conocimiento no supondrá, en ningún caso, una modificación de este punto.
9. Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle.
10. La seguridad de los Datos de Carácter Personal albergados en ficheros automatizados, el personal que pertenece a empresas proveedoras de servicios, observen las siguientes normas de actuación, además de las consideraciones ya mencionadas:
    a. El personal sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de los puestos (ordenadores personales) del personal y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

b. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable de dicha información o fichero.
c. El propietario de la información se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

d. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

7.7.3 Control de acceso físico a instalaciones.

1. El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión. Se limitará el acceso al personal de soporte externo a las áreas especialmente protegidas. Este acceso, como el de cualquier otra persona ajena que requiera acceder a áreas protegidas, se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado. El sistema de control mantendrá un registro de todos los accesos de personas ajenas.
2. Se acompañará a los visitantes en áreas protegidas y el sistema
registrará la fecha y hora de su entrada y salida. Dichas personas deberán ir provistos de la debida tarjeta de identificación o permiso correspondiente y pasar por alguno de los sistemas de control de acceso físico. Sólo se permitirá el acceso previa identificación de la persona de contacto.

7.7.4 Uso apropiado de los recursos

Los recursos a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para complementar las obligaciones y propósito de la operatividad para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso. Queda terminantemente prohibido:

1. El uso de estos recursos para actividades no relacionadas con el propósito del servicio, o bien la extralimitación en su uso.

2. La búsqueda o explotación de vulnerabilidades en cualquier aplicación o equipos.
3. Los equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios de la compañía o bajo supervisión de la Dirección de TI.
4. Introducir en los sistemas de información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
5. Introducir voluntariamente cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. El proveedor tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
6. Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
7. Intentar acceder a áreas restringidas de los sistemas de información sin la debida autorización.
8. Intentar distorsionar o falsear los registros “log” de los sistemas de información.
9. Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos.
10. Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, dañar o alterar los recursos informáticos.
11. Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos. Estos actos podrían constituir un delito de daños, según la legislación vigente.
12. Albergar datos de carácter personal en las unidades locales de disco de los puestos (ordenadores personales) de usuario.
13. Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

14. Conectar ordenadores no corporativos a la red de comunicaciones, disponibles para visitas, proveedores, etc. que necesiten de una conexión con acceso a Internet.

7.7.5 Protección frente a malware

Los recursos que el proveedor utiliza para la prestación del servicio deberán seguir las siguientes indicaciones:

1. Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles.
2. El software antivirus se deberá instalar y usar en todos los servidores, en su caso, y en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
3. El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los ficheros de definición de virus tanto en los ordenadores personales como servidores, en su caso, así como de bloqueo frente a la detección de virus informáticos.
4. Todo el software debe estar correctamente licenciado por lo que se prohíbe expresamente el uso de software pirata, crackers, etc.
5. En caso de que sea detectado cualquier malware en uno de los equipos conectados será desconectado de dicha red sin que sea necesario aviso previo. El área de Seguridad notificará con los medios disponibles el problema encontrado por lo que será responsabilidad de la contrata la eliminación del malware detectado. La conexión de nuevo a la red corporativa debe ser autorizada por el área de Seguridad Lógica, la cual solicitará toda la información necesaria sobre el equipo con el fin de asegurar la limpieza de este.

7.7.6 Normas para Intercambio de información

1. Los usuarios no deben ocultar o manipular su identidad en ninguna circunstancia.
2. En los casos en que la Dirección de TI asigne un usuario genérico, será responsabilidad del proveedor mantener una relación actualizada de las personas que utilizan dicho usuario genérico en cada momento.
3. La distribución de información ya sea en formato digital o papel se realizará mediante los dispositivos facilitados por la compañía, para tal cometido y con la finalidad exclusiva de facilitar las funciones del puesto. La Dirección de TI se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos dispositivos de difusión.

4. En relación con el intercambio de información, se considerarán no autorizadas las siguientes actividades:
5. Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
6. Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
7. Transferencia de ficheros a terceras partes no autorizadas de material que es de alguna u otra manera confidencial.
8. Transmisión o recepción de ficheros que infrinjan la Ley de Protección de Datos de Carácter Personal.
9. Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
10. Participación en actividades de Internet como grupos de noticias, juegos, apuestas u otras que no estén directamente relacionadas con el negocio.
11. Todas las actividades que puedan dañar la buena reputación prohibidas en Internet y en cualquier otro lugar. Esto se refiere también a actividades realizadas para el propio beneficio económico del usuario o de terceras partes, y a actividades de naturaleza política.
12. Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo podrá ser realizada por personal autorizado y con el debido permiso.
13. Si el tratamiento de datos de carácter personal se llevase a cabo fuera de los locales donde está ubicado el fichero, dicho tratamiento deberá ser autorizado expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
14. La transmisión de datos de carácter personal de nivel alto a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

7.7.7 Criterios de uso del correo electrónico

La cuenta de correo electrónico tiene la consideración de herramienta que el contratista debe aportar para el desempeño de los trabajos contratados, a continuación, se presentan una serie de reglas sugeridas:

1. Cada usuario de los sistemas informáticos dispondrá de una cuenta de correo electrónico específica y única, asignada exclusivamente a dicho usuario.
2. Los usuarios externos no dispondrán de una dirección de correo del grupo (dominio @empresa.com, @empresa.com.sv…).
3. En el momento de su registro, el usuario externo debe aportar una dirección de correo del dominio de su propia empresa o bien una dirección de correo personal.
4. Este criterio general es compatible con el hecho de que dichos usuarios pueden acceder a los buzones de correo genérico que sean preciso para desarrollar su operativa de trabajo. El envío de correos desde estos buzones genéricos no identifica al emisor.
5. El sistema de correo electrónico no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
6. Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o difusiones generalizadas (mensajes que se extienden a múltiples usuarios).
7. No está permitida la transmisión vía correo electrónico de información que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío esté permitido.
8. No está permitida la transmisión vía correo electrónico de información confidencial salvo que la comunicación electrónica esté bien cifrada y el envío esté permitido.

7.7.8 Normas para la conectividad a Internet

1. Los usuarios no deben buscar o visitar sitios que no sirvan como soporte al servicio prestado.
2. Todo el tráfico desde y hacia Internet será inspeccionado en búsqueda de amenazas. En caso de que algún equipo se encuentre accediendo a sitios clasificados como maliciosos (pornografía, juego, etc.) o ajenos al negocio podrá ser desconectado de la red sin que sea necesario aviso previo.
3. La empresa puede reservarse el derecho de, en lo permitido por el marco legal, y sin aviso previo, limitar el acceso total o parcial a Internet a partir de la red informática y terminales.
4. El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporados en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.

5. Los usuarios no deberán usar el nombre, símbolo, logotipo de la empresa o símbolos similares en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
6. Únicamente se permitirá la transferencia de datos de o a Internet en conexión con las actividades del servicio prestado la Dirección de TI. La transferencia de ficheros no relativa a estas actividades (por ejemplo, la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia) está prohibida, quedando expresamente prohibido el uso de software tipo P2P o torrents.

7.7.9 Responsabilidades del usuario

Todo usuario externo, por el hecho de serlo, asume determinadas responsabilidades:

1. Cada usuario será responsable de su identificador y todo lo que de él se derive, por lo que es imprescindible que este sea únicamente conocido por el propio usuario; no deberá revelarlo al resto de usuarios bajo ningún concepto.
2. El usuario será responsable de todas las acciones registradas en los sistemas informáticos con su identificador.
3. Los usuarios deberán seguir las directivas definidas con relación a la gestión de las contraseñas.
4. Los usuarios deberán asegurar que los equipos quedan protegidos cuando estén desatendidos.
5. Se establecerán las siguientes políticas de escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
   5.1 Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
   5.2 No dejar desatendidos los equipos asignados a funciones críticas y bloquear su acceso cuando sea estrictamente necesario.
   5.3 Asegurar la confidencialidad de los documentos tanto en los puntos recepción y envío de información (correo postal, máquinas de escáner y fax) como en los equipos de duplicado (fotocopiadora, fax y escáner).
6. La reproducción o envío de información con este tipo de dispositivos queda bajo la responsabilidad del usuario.

7. Los listados con datos de carácter personal o información confidencial deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
8. Los listados con datos de carácter personal o información confidencial deberán eliminarse de manera segura una vez no sean necesarios.
9. En caso de identificarse incidentes o debilidades relacionadas con la seguridad de la información, se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar esta supuesta debilidad o incidente de seguridad.

7.7.10 Equipos de Usuarios

Sobre el equipamiento informático asociado al puesto del usuario se establecen los siguientes principios:

1. Todos los puestos de usuario con conectividad a recursos informáticos estarán controlados por la Empresa
2. Ningún usuario intentará por ningún medio transgredir el sistema de seguridad y las autorizaciones, ni dispondrá de herramientas que puedan realizarlo.
3. Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas por el área de Seguridad de la Empresa.
4. Cuando se desatienda un puesto durante un periodo corto de tiempo el usuario deberá activar su bloqueo. Cuando se termina la jornada de trabajo se debe apagar el equipo.

7.7.11 Identificadores de usuario y contraseñas

El personal de empresas proveedoras de servicios que accede a los sistemas de información dentro de su ámbito de trabajo, es responsable de asegurar que los datos, las aplicaciones y los recursos informáticos sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados e implantados. Este personal está obligado a utilizar los recursos y los datos contenidos en ellos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales. Para obtener el acceso a los sistemas de información este personal debe disponer de un acceso autorizado (identificador de usuario y contraseña) sobre el que, como usuarios de sistemas de información, deben observar los siguientes principios de actuación y buenas prácticas:

1. Cuando el usuario recibe su identificador de acceso a los sistemas se considera que acepta formalmente la Política de Seguridad vigente.

2. Los usuarios deben mantener sus credenciales de acceso confidenciales.
3. Todos los usuarios con acceso a un sistema de información dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
4. Los intentos de logue sin éxito son limitados en número.
5. Todos los intentos de logue son registrados, tanto tengan éxito o no.
6. Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
7. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
8. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
9. Los usuarios no deben incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
10. Las contraseñas estarán constituidas por combinación de caracteres alfabéticos y numéricos. Todo lo relacionado con las contraseñas de usuario se encuentra recogido en la IT “Gestión de contraseñas”.
11. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista ni al alcance de terceros.
12. Los usuarios no deben utilizar las mismas contraseñas para uso personal y profesional.
13. Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
14. Con relación a datos de carácter personal, exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.
15. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder de inmediato al cambio de su contraseña para notificar la incidencia.
16. El cambio de la contraseña se realizará en el sistema de gestión de accesos de la Empresa.

7.7.12 Software.

Sobre el software se establecen los siguientes principios:

1. La Empresa facilitará al proveedor un documento que incluirá directrices a seguir en relación con el software de los equipos ("Conexión de Empresas Colaboradoras a la red de datos)".
2. Todo el personal que accede a los sistemas de información debe utilizar únicamente las versiones de software indicadas y siguiendo sus normas de utilización.
3. Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.
4. Se prohíbe el uso de software no validado.
5. Se prohíbe el uso de software sin su respectiva licencia.
6. Se prohíbe el uso de software crackeado o pirateado.

7.7.13 Conexión a la red

Sobre la conexión a la red se establecen los siguientes principios:

1. En caso de que el proveedor necesite acceder a la red para la prestación de los servicios, debe solicitar el documento "Conexión de Empresas Colaboradoras a la red de datos de la Empresa" a la dirección de correo, identificando la empresa, persona de contacto y propuesta a la que opta.
2. El acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación previa validación del acceso.
3. La Empresa se reserva el derecho de, sin aviso previo, bloquear, suspender, alterar o monitorizar los servicios soportados en su red informática y puestos a disposición de las entidades externas.
4. No se deberá conectar a ninguno de los recursos ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas a la red corporativa.
5. Nadie deberá conectarse a la red corporativa a través de otros medios que no sean los definidos.
6. La Empresa se reserva el derecho a desconectar de la red corporativa y sin aviso previo a cualquier equipo utilizado por un proveedor cuando se detecten actividades que contravengan los principios y normas expresados en el presente documento.

7.7.14 Gestión de accesos

Existe un proceso formal para el registro, concesión, alteración y revocación de accesos a los usuarios, aplicable a todos los sistemas de Información de la Empresa. Se establecen los siguientes principios:

1. Existe un proceso formal para la gestión de los accesos de los usuarios a los sistemas.
2. Se debe asegurar la comunicación de las reglas y responsabilidades en el uso de los sistemas de información de la Empresa a los usuarios al atribuirles cualquier acceso a los sistemas.
3. Para cada sistema existe un conjunto de perfiles y privilegios que se atribuyen a los usuarios de acuerdo con sus necesidades.
4. Los privilegios de acceso a los sistemas se atribuyen a los usuarios considerando las necesidades efectivas para el desempeño de sus funciones, no debiendo ser atribuidos ni por exceso ni por defecto.
5. Los sistemas de la Empresa, por omisión, bloquean el acceso a los usuarios no autorizados.
6. Los privilegios de acceso a los sistemas garantizan una correcta segregación de funciones. En los casos en los que no es posible garantizar la segregación de funciones, están implementados los controles compensatorios adecuados.
7. Cualquier solicitud de atribución o modificación de privilegios de acceso a los sistemas de la Empresa se refleja en la herramienta de gestión de identidades y accesos y posteriormente debe ser aprobada.
8. Los accesos y respectivos privilegios solo se implementan en los sistemas después de obtener todas las aprobaciones necesarias.
9. Se mantiene un registro formal de todos los usuarios autorizados y respectivos privilegios de acceso a los sistemas de la Empresa.
10. Las modificaciones en las necesidades de acceso a los sistemas deben llevar aparejados los ajustes a los derechos de acceso.
11. Los privilegios de acceso a los sistemas atribuidos a los usuarios son revocados de forma automática cuando termina su relación profesional con la Empresa.
12. Se realiza una revisión periódica con el fin de eliminar o bloquear cuentas redundantes o innecesarias.
13. Los usuarios deben tener asociados, identificadores individuales (ID de usuario), protegidos por contraseña.
14. El uso de identificadores genéricos (cuentas genéricas o de grupo) se debe permitir solo en casos excepcionales debidamente justificados, aprobados y registrados.
15. Las cuentas genéricas tienen asociado un usuario individual responsable de esa cuenta.

16. La nomenclatura utilizada en la generación de los identificadores obedece a reglas definidas por la Empresa.
17. El identificador de usuario permite reconocer su identidad, pero nunca sus niveles de privilegios.
18. El identificador debe ser personal, de uso exclusivo y único para todos los sistemas (cuando sea técnicamente viable).
19. Los identificadores de los usuarios que ya no tienen vínculo con la Empresa no pueden ser atribuidos a otros usuarios, excepto en áreas de gran rotación de personas (por ejemplo, el centro de contactos).
20. En los casos de áreas de gran rotación referidas en el punto anterior, debe existir una aprobación formal de la excepción por el responsable del área.
21. Para las excepciones debe quedar registrado y mantenido un histórico de las personas asociadas a un ID de usuario y el tiempo que durado dicha asociación (fechas de inicio y de fin).
22. La Empresa se reserva el derecho de, sin aviso previo, bloquear, suspender, modificar y monitorizar a los usuarios de sus sistemas y los respectivos privilegios de acceso.
23. El responsable de contratar debe notificar, todos los cambios habidos en cuanto a las personas, identidades y equipos que estén conectados a la red corporativa. Además, el responsable de la Empresa tiene la obligación de comunicar esta información al área de Seguridad, el cual mantendrá un inventario actualizado de las conexiones realizadas a la red corporativa por los contratos.

7.7.15 Propiedad intelectual

Con relación a la Propiedad Intelectual se aplicarán los siguientes principios:

1. Las entidades externas que acceden a Internet a partir de la red informática y terminales de la empresa son responsables de respetar los derechos de propiedad intelectual aplicables a los contenidos accedidos.
2. Los usuarios externos únicamente podrán utilizar material autorizado para el desarrollo de sus funciones.
3. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia.
4. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

5. La empresa únicamente autorizará el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

7.7.16 Incidencias

En el caso de detectarse alguna incidencia relacionada con los sistemas de información se seguirán las siguientes normas:

1. Todo el personal externo deberá ponerse en contacto con el servicio del centro de atención al usuario en caso de que detecte cualquier incidencia relacionada con la información o los recursos informáticos.
2. Cualquier usuario podrá trasladar las sugerencias y/o debilidades, que pueda tener relación con la seguridad de la información y las directrices contempladas en la presente Política.
3. Se deberá notificar cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.
4. El centro de atención al usuario de la empresa centraliza la recogida, análisis y gestión de las incidencias recibidas.

7.7.17 Requisitos de seguridad para la externalización (para terceros)

El literal 6.2 terceros, de la norma ISO 27002:2013 nos dice que para mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización para que sean accesibles por terceros, la seguridad de la información de la empresa y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo, debería controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización, si el negocio requiera dicho acceso de terceros, se debería realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad si se requieren medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.

La empresa debe de elaborar inventario de conexiones de red y flujos de información significativos con 3as partes, para que evalúe sus riesgos y revise los controles de seguridad de información existentes respecto a los requisitos.

Es de considerar exigir certificados en ISO/IEC 27001 a los partners más críticos, tales como outsourcing de TI, proveedores de servicios de seguridad TI, etc.

Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras. Ejemplo:

1. Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.
2. Se deberían anexar todos los requisitos identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización.
3. Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la empresa o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.

7.7.18 Exigencias (La Empresa se reserva el derecho de exigir)

1. La implementación de cualquier mecanismo que considere necesario para garantizar la seguridad de acceso a sus datos y activos. Así mismo podrá exigir las penalizaciones y/o las garantías apropiadas en función de los riesgos de incumplimiento o deterioro de los activos del servicio.

2. La presencia y colaboración, de todas las empresas colaboradoras y proveedoras y su mejor ayuda en la restauración –bajo la coordinación directa de la actividad normal de sus operaciones de negocio, después de que éstas hayan sido interrumpidas por una emergencia o desastre.

3. La tenencia de políticas y planes de continuidad de negocio o contingencias que permitan asegurar la continuidad de las actividades de estas compañías en el caso de que se vieran afectadas por una catástrofe o situación de desastre. De igual forma, se reserva el derecho de auditar la existencia y grado de implantación de los mencionados planes.

7.7.19 Privacy by design (Privacidad por diseño)

La privacidad por diseño consiste en nada más que protección de datos mediante diseño de tecnología. Detrás de esto está la idea de que la

protección de datos en procedimientos de procesamiento de datos se cumple mejor cuando ya está integrada en la tecnología cuando se creó. Por lo que Privacidad por diseño posee siete principios los cuales son los siguientes:

1. Proactivo no retroactivo, es decir preventivo no correctivo. La privacidad, por diseño, no espera a que se materialicen los riesgos de privacidad, ni ofrece remedios para resolver las infracciones de privacidad una vez que se han producido, sino que pretende evitar que ocurran.
2. Privacidad como configuración predeterminada. Busca entregar el máximo grado de privacidad al garantizar que los datos personales estén automáticamente protegidos en cualquier sistema de TI.
3. Privacidad integrada en el diseño. La privacidad por diseño está integrada en el diseño y la arquitectura de los sistemas de TI y las prácticas comerciales, como resultado se tiene que la privacidad se convierte en un componente esencial de la funcionalidad principal que se entrega sin disminuir la funcionalidad.
4. Funcionalidad completa: suma positiva, busca acomodar todos los intereses y objetivos legítimos en una forma positiva de "ganar-ganar".
5. Seguridad de extremo a extremo: protección completa del ciclo de vida, esto garantiza que todos los datos se retengan de forma segura y luego se destruyan de forma segura al final del proceso, de manera oportuna.
6. Visibilidad y transparencia: manteniéndolo abierto. La privacidad por diseño busca asegurar a todos los interesados que cualquiera que sea la práctica tecnológica involucrada, siempre esté operando de acuerdo a los objetivos establecidos y que sean estas operaciones transparentes y visibles tanto para usuarios y proveedores.
7. Respeto a la privacidad del usuario: la privacidad por diseño requiere que los arquitectos y operadores mantengan los intereses de la persona y manteniendo la privacidad de este.

7.8. Gestión de incidentes de seguridad de la información.

Cuando se habla de la gestión de incidentes, la norma hace referencia con recomendaciones relacionadas con la notificación de eventos y puntos débiles de seguridad de la información y los procedimientos y responsabilidades que se deberían asignar para la gestión de incidentes y mejoras de seguridad de la información.

Se tiene que reducir el impacto en las operaciones empresariales y asegurar un servicio de la mejor calidad posible. Es fundamental conocer las causas del incidente, lo cual podría requerir un análisis de causa raíz para comprenderlas mejor y tomar las medidas necesarias.

Para recuperar el servicio, hace falta implementar rápidamente una solución o una alternativa.
Se puede iniciar por registrar los incidentes con diferentes métodos (directamente en el portal de autoservicio, en llamadas telefónicas, chats, correos electrónicos, en la interfaz web o en eventos entrantes). Esos incidentes se priorizan y asignan en función del impacto y la urgencia de la falla o la interrupción. Luego se puede automatizar ese proceso y enviarlos directamente a los agentes o equipos de soporte correspondientes. Esto permite ahorrar tiempo a todos y disminuye los tickets creando una base de conocimientos con todas las preguntas frecuentes y soluciones posibles.
Más allá de las herramientas es muy importante tener definidas las acciones y los roles que deben desempeñar todos los empleados de una compañía cuando se presente un incidente, para de esta forma establecer las medidas correctivas necesarias para que no se vuelvan a presentar.

7.8.1 El diagnóstico correcto cuando se gestionan incidentes.

El primer paso para gestionar un incidente es diagnosticar. Se debe analizar y determinar el impacto, y también el síntoma para detectar. Agregar los problemas a las notas para averiguar las causas y establecer medidas para rectificarlos. Una vez realizado el análisis de causa raíz, se puede encontrar una alternativa simple.

7.8.2 Acuerdo de nivel de servicio.

El acuerdo de nivel de servicio hace referencia al plazo que se designa para que cada agente responda a los incidentes y resuelva los tickets en función de sus prioridades. Esto te permite determinar qué problemas son críticos y escalarlos oportunamente. Aplica normas rigurosas de desempeño para tu equipo de soporte, a fin de satisfacer las solicitudes de los clientes.

7.8.3 Cierre automático

Puede crear un conjunto de reglas y cierra automáticamente todos los tickets resueltos. La interrelación de incidentes y problemas específicos se simplifica gracias a la automatización del servicio de ayuda, lo que mejora la productividad del soporte para los clientes.

7.8.4 Encuesta de satisfacción de los usuarios

Consiste en identificar el nivel de satisfacción de los usuarios y evalúa el desempeño de los agentes de soporte a la hora de resolver problemas. ¿Cómo hacerlo? Con un simple formulario de encuesta que se envía tras el cierre del ticket. Luego se miden los resultados y se trata de mejorarlos.

7.8.5 Gestión de incidentes y data breach

Consiste en políticas y procedimientos, un sistema de control interno más riguroso y un comité de auditoría independiente, es la manera más efectiva de minimizar los riesgos asociados al fraude corporativo. Este monitoreo y control se puede realizar mediante el incremento de los controles internos de las empresas, y la implementación de medidas preventivas que garanticen la integridad y precisión de sus informes financieros, esto mediante formularios 20-F de la ley SOX (Ver Anexo 1), para la regulación financiera y evitar que se realicen fraudes constantes en los procesos de las operaciones o transacciones.

7.9. Gestión de la continuidad del negocio

La Gestión de la Continuidad del Negocio (también llamada BCM, por sus siglas en inglés) es el proceso de lograr esta capacidad y mantenerla, y conforma una parte vital de la gestión de seguridad de sistemas de información, que ahora se conoce más comúnmente como seguridad cibernética.

La continuidad del negocio no es sólo para TI, la mayoría de las organizaciones de hoy son sumamente dependientes de la tecnología de la información (desde equipos portátiles hasta servidores, de escritorio hasta tabletas y smartphones), pero queda claro que esta tecnología puede verse afectada por una amplia gama de incidentes potencialmente desastrosos. Éstos van desde cortes en el suministro de energía provocados por tormentas hasta la pérdida de datos causada por equivocaciones de los empleados o por criminales informáticos.

Desafortunadamente, algunas empresas deben cerrar cuando las alcanza un desastre para el cual no estaban preparadas adecuadamente. Es lamentable porque el camino para dicha preparación está bien documentado. Cualquier empresa de cualquier tamaño puede mejorar las posibilidades de superar un incidente de interrupción de la actividad y quedar en una pieza (con la marca intacta y sin merma en los ingresos) si sigue ciertas estrategias probadas y de confianza, más allá de que desee obtener la certificación ISO o no.
A continuación, un resumen de los cuatro pasos principales:

7.9.1. Identificar y ordenar las amenazas.

Crea una lista de los incidentes de interrupción de la actividad que constituyan las amenazas más probables para la empresa. No se recomienda utilizar la lista de otro, porque las amenazas varían según la ubicación. Por ejemplo, si en la zona donde se encuentra la organización hay un grado relativamente alto de sensibilización con respecto a los terremotos, incendios forestales, etc. Sería recomendable llevar a cabo un nivel básico de planificación para estar preparados ante desastres teniendo esos eventos en cuenta.

Para identificar las amenazas, se podría iniciar contestando preguntas como las siguientes: ¿Qué pasa con la fuga de datos o la interrupción de la infraestructura de TI, que pueden ocurrir en cualquier parte? ¿Qué pasa si un producto químico tóxico provoca que se cierren las instalaciones por varios días? ¿La organización está ubicada cerca de un aeropuerto? ¿De una autopista importante? ¿Cuánto depende la empresa de proveedores extranjeros?

En esta etapa, una buena técnica es reunir personas de todos los departamentos en una sesión de intercambio de ideas. El objetivo de la reunión es crear una lista de escenarios ordenados por probabilidad de ocurrencia y por potencial de causar un impacto negativo.

7.9.2. Realizar un análisis del impacto en la empresa.

Determinar qué partes de la organización son las más críticas para que sobreviva. Una manera es comenzar detallando las funciones, los procesos, los empleados, los lugares y los sistemas que son críticos para el funcionamiento de la organización. De esto se puede ocupar el líder del proyecto de gestión de la continuidad del negocio; para ello, podría entrevistar a los empleados de cada departamento y luego elaborar una tabla de resultados que liste las funciones, las personas principales y las secundarias.

A continuación, determinar la cantidad de “días de supervivencia” de la empresa para cada función. ¿Cuánto puede resistir la empresa sin que una función en particular provoque un impacto grave?

Luego, ordenar el impacto de cada función en caso de que no esté disponible. Por ejemplo, expertos en recuperación ante desastres, sugiere utilizar una escala de 1 a 4, donde 1 = impacto crítico en las actividades operativas o pérdida fiscal, y 4 = sin impacto a corto plazo. Si luego se multiplica el Impacto por los “días de supervivencia”, se puede ver cuáles son las funciones más críticas. Al principio de la tabla quedarán las funciones con un impacto mayor y con sólo un día de supervivencia.

7.9.3. Crear un plan de respuesta y recuperación

En esta etapa se clasifican datos claves sobre los bienes involucrados en la realización de las funciones críticas, incluyendo sistemas de TI, personal, instalaciones, proveedores y clientes. Se incluyen números de serie de los equipos, acuerdos de licencia, alquileres, garantías, detalles de contactos, etc.

Se necesita determinar “a quién llamar”; en cada categoría de incidente y crear un árbol de números telefónicos para que se hagan las llamadas correctas en el orden correcto. También es útil una lista de “quién puede decir qué cosa” para controlar la interacción con los medios durante un incidente (se puede considerar quedarse con una estrategia de “sólo el CEO” si se trata de un incidente delicado).

Es recomendable documentar todos los acuerdos vigentes para mudar las operaciones a ubicaciones e instalaciones de TI temporales, de ser necesario. No olvidar documentar el proceso de notificación para los miembros de la empresa en su totalidad y el procedimiento de asesoramiento para clientes.

Los pasos para recuperar las operaciones principales deberían ordenarse en una secuencia donde queden explícitas las interdependencias funcionales. Cuando el plan esté listo, asegúrate de capacitar a los gerentes sobre los detalles relevantes para cada departamento, así como la importancia del plan general para sobrevivir a un incidente.

7.9.4. Prueba del plan y refinamiento del análisis

Se recomienda probar el plan al menos una vez al año, con ejercicios, análisis paso a paso o simulaciones. La prueba permite sacar el mayor provecho a lo que se ha invertido en la creación del plan, y no sólo permite encontrar fallas y dar cuenta de los cambios corporativos con el transcurso del tiempo, sino que también causa una buena impresión en la gerencia.

Si el proyecto parece demasiado desalentador para aplicar a la empresa completa, se puede considerar comenzar por unos pocos departamentos o una sola oficina, si hay varias. Todo lo que se vaya aprendiendo en el proceso se podrá aplicar en mayor escala a medida que se progrese. Se debe de evitar a toda costa pensar que las cosas malas no suceden, porque sí lo hacen. Sólo se tiene que estar preparado. Y no se debe de pretender que cuando ocurra algo no será tan malo, porque podría llegar a serlo.

8. Conclusiones

Como resultado a la investigación realizada es posible concluir que en la actualidad la seguridad de la información de una empresa está expuesta a diferentes tipos de amenazas que existen en el ámbito de la tecnología, debido a esto existen una gran cantidad de procedimientos, normativa y estándares disponibles para la protección de los datos, y a las dificultades técnicas inherentes a la informática, por lo que resulta difícil para los recursos humanos del área de tecnología encontrar una referencia o documento que reúna las buenas prácticas de seguridad informática en el tratamiento de datos.

Además, las amenazas de seguridad a las que se están enfrentando las organizaciones no son vulnerabilidades nada fáciles, y su control depende en gran medida de la política de seguridad de la organización. Así como también la formación de cada uno de los trabajadores en materia de seguridad y privacidad de la información es crucial para evitar errores que comprometan el sistema informático de la organización. Por lo tanto, es de vital importancia vigilar y actualizar los hábitos de seguridad del personal con acceso a los sistemas informáticos de la organización.

La guía presentada en este trabajo pretende ser una orientación sobre buenas prácticas y hábitos del personal en el tratamiento de los datos, y ayudar en la formación de estos profesionales para que posean además de todas las normas y buenas prácticas existentes, un recurso que les aporte el conocimiento de estos dos aspectos combinados para la implementación del área de seguridad de la información.

Es necesario cambiar la actitud y comportamiento de las personas que manejan esquemas del pasado, porque las capacidades individuales y colectivas son el principal activo de la empresa para competir. Las exigencias de un mercado en continuo cambio superan y tensionan los procesos organizados de forma tradicional.

El modelo de madurez se basa en áreas que normalmente manejan las empresas y elementos que son los generadores del cambio, lo cual se enmarca en cuatro niveles que se resumen de la siguiente forma (ver figura 8).

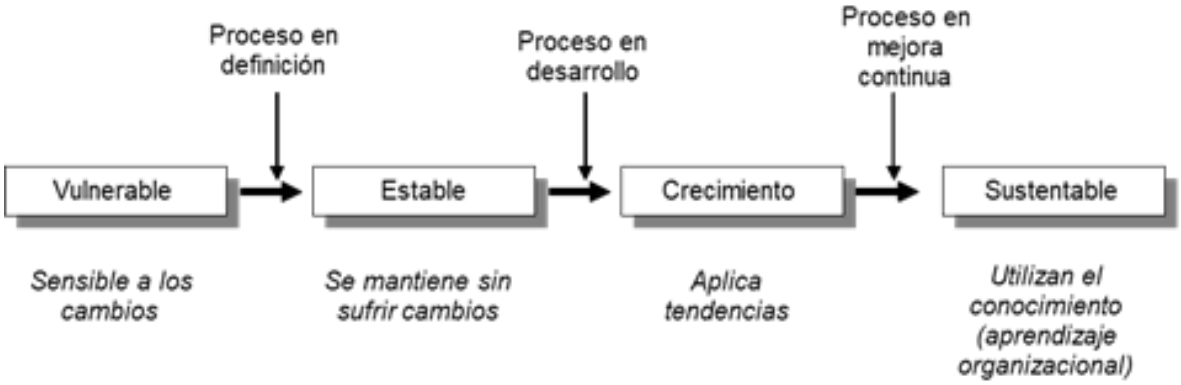

Figura. 8. Niveles aplicables al modelo de madurez

Modelo que identifica el nivel de madurez de los procesos de las empresas.

El nivel de competitividad de las empresas se fundamenta en su capacidad y se mide de acuerdo al proceso de evolución en la competitividad.
El proceso evolutivo que posiciona el nivel de competitividad, se basa en sus prácticas establecidas en todas sus áreas, de acuerdo a características que reflejan sus capacidades. Este proceso evolutivo expone el tipo de prácticas predominantes, que parten de un nivel elemental (nivel vulnerable) y se desplazan hacia mejores prácticas que corresponden a estándares de sustentabilidad.

9. Glosario

A

Activos informáticos: Son los recursos (hardware y software) con los que cuenta una empresa

Amenaza: surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

C

Ciberdelincuente: son personas que realizan actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.

COBIT: Objetivos de control para la información y tecnologías relacionadas, es una metodología publicada en 1996 por el instituto de Control de TI y la ISACA que se usa para evaluar el departamento de informática de una compañía.

Control de Acceso: es el proceso de conceder o denegar permisos a usuarios o grupos de acceso a un recurso particular de una entidad en particular.

Copyright: derecho exclusivo de un autor, editor o concesionario para explotar una obra literaria, científica o artística durante cierto tiempo.

Crackear: se utiliza para referirse a las personas que rompen o explotan la vulnerabilidad algún Sistema de seguridad, que pueden realizarlo por diferentes razones incluyendo fines de lucro, protestas, etc.

Criptografía: es la técnica para asegurar la transmisión de información privada que utiliza una escritura convencional secreta, de manera que sea ilegible para cualquiera que no posea la clave de descifrado.

E

Exploit: es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad (bug) del Sistema.

I

ICS: conexión compartida a Internet (Internet Connection Sharing)

IPS: Sistema de **p**revención de **I**ntrusos.

ITIL: Information **T**echnology **I**nfrastructure **L**ibrary.

IT: **I**nformation **T**echnology.

L

Log: grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso en particular.

LOPD: Ley de **P**rotección de **D**atos.

LSSI: Ley de **S**ervicios de la **S**ociedad de la **I**nformación y de **C**omercio **E**lectrónico.

M

Malware: códigos diseñados por ciberdelincuentes cuyo objetivo es el de variar el funcionamiento de cualquier sistema informático, sobre todo sin el usuario se dé cuenta.

N

Norma ISO: norma definida por la **O**rganización **I**nternacional de **N**ormalización que se aplica a los productos y servicios.

P

Phishing: es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

R

Riesgo informático: probabilidad que se manifieste un evento natural o provocado.

S

Seguridad de la información: conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de datos y de la misma.

Software: conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Spectre: es una vulnerabilidad que afecta a los microprocesadores modernos que utilizan predicción de saltos.

SLA: Service Level Agreement (Acuerdos de Nivel de Servicio).

U

UC: User Contract (Contrato de Apoyo).

V

Vulnerabilidad: es una debilidad del sistema informático que puede ser utilizada para causar daño.

10. Referencias

ISACA. (2012). *COBIT 5 Procesos Catalizadores.*

NORMA TÉCNICA SALVADOREÑA. (2013). *Tecnología de la información - Técnicas de seguridad - Sistema de gestión de seguridad de la información - Requisitos.* NTS ISO/IEC 27001:2013*.*

NORMA TÉCNICA SALVADOREÑA. (2013). *Tecnología de la información.Código de prácticas para la gestión de la seguridad de la información.* NTS ISO/IEC 27002:2013*.*

ITIL. (2011). *ITIL Service Design v4.*

Pesante, L. (2008). *Introduction to Information Security.* Obtenido de US-CERT: https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf

Tomás Foltýn. (2017). *Resumen de seguridad 2017: El año de los llamados de atención Parte 1.* Obtenido de WeLiveSecurity by ESET: https://www.welivesecurity.com/la-es/2017/12/29/resumen-seguridad-2017-parte-1/

Tomás Foltýn. (2018). *Resumen de seguridad 2017: El año de los llamados de atención Parte 2.* Obtenido de WeLiveSecurity by ESET: https://www.welivesecurity.com/la-es/2017/12/29/resumen-seguridad-2017-parte-2/

11. Anexos

ANEXO 1. FORMULARIO 20-F SOX

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORMULARIO 20-F

DECLARACIÓN DE REGISTRO EN CONFORMIDAD CON LO DISPUESTO EN LA SECCIÓN 12(b) O 12(g) DE LA LEY DE BOLSAS DE 1934

o

INFORME ANUAL EN CONFORMIDAD CON LO DISPUESTO EN LA SECCIÓN 13 O 15(d) DE LA LEY DE BOLSAS DE 1934

o

INFORME DE TRANSICIÓN EN CONFORMIDAD CON LO DISPUESTO EN LA SECCIÓN 13 O 15(d) DE LA LEY DE BOLSAS DE 1934

o

MEMORIA CORPORATIVA DE SOCIEDAD INSTRUMENTAL EN CONFORMIDAD CON LO DISPUESTO EN LA SECCIÓN 13 O 15(d) DE LA LEY DE BOLSAS DE 1934

Fecha del evento que exige la presentación de esta memoria corporativa de sociedad instrumental

Número de expediente de la Comisión:

(Nombre exacto del Registrante tal como aparece en su escritura de constitución)

(Traducción al inglés del nombre del Registrante)

(Jurisdicción de constitución u organización)

(Dirección de la sede corporativa principal)

(Nombre, número de teléfono, correo electrónico y/o fax y dirección de Persona de Contacto de la Compañía)

Valores registrados o a ser registrados en conformidad con lo dispuesto en la Sección 12(b) de la Ley:

Denominación de cada clase	**Nombre de cada Bolsa de Valores en las que están registrados**

* Valores registrados, no para ser comercializados, sino sólo en relación con el registro de los American Depositary Shares, según lo dispuesto por la Securities and Exchange Commission.

Valores registrados o a ser registrados en conformidad con lo dispuesto en la Sección 12(g) de la Ley: No hay
Valores registrados respecto de los cuales existe una obligación de informar en conformidad con lo dispuesto en la Sección 15(d) de la Ley: No hay

Marque en el recuadro que corresponda si la entidad registrante constituye una emisora acreditada conocida, a tenor de la definición contemplada en la Regla 405 de la Ley de Valores. ☒ Sí No

Si el presente informe constituye un informe anual o de transición, marque en el recuadro que corresponda si la entidad registrante se exime o no presentar los informes en conformidad con la Sección 13 o 15(d) de la Ley de Bolsas de 1934. Sí ☒ No

Marque en el recuadro que corresponda si la entidad registrante (1) ha presentado todos los informes que la Sección 13 o 15(d) de la Ley de Bolsas de 1934 exige presentar durante los 12 meses precedentes (o período menor durante el cual la entidad registrante haya tenido la obligación de presentar tales informes) y (2) ha estado sujeta a dichos requisitos de presentación en los últimos 90 días. ☒ Sí No

Marque en el recuadro que corresponda si la entidad registrante ha presentado electrónicamente o publicado en su página web corporativa, de tenerla, la totalidad de los Archivos de Datos Interactivos que está obligada a presentar y publicar en conformidad con la Regla 405 del Reglamento S-T durante los doce meses precedentes (o período menor durante el cual la entidad registrante haya tenido la obligación de presentar y publicar tales archivos). ☒ Sí No

Marque en el recuadro que corresponda si la entidad registrante es un registrante acelerado grande, un registrante acelerado, un registrante no acelerado o una empresa de crecimiento emergente. Véase las definiciones de "registrante acelerado grande", "registrante acelerado" y "empresa de crecimiento emergente" en la Regla 12b-2 de la Ley de Bolsas.

Registrante acelerado grande ☒ Registrante acelerado ☐ Registrante no acelerado ☐ Empresa de crecimiento emergente ☐

Si el registrante es una empresa de crecimiento suficiente que prepara sus estados financieros en conformidad con los PCGA estadounidenses (U.S. GAAP), marque el recuadro si el registrante ha optado por no usar el período de transición ampliado para dar cumplimiento a normas de contabilidad financiera nuevas o revisadas † que contempla la Sección 13(a) de la Ley de Bolsas. ☐

† El término "norma de contabilidad financiera nueva o revisada" se refiere a cualquier actualización dictada por el Consejo de Normas Internacionales de Contabilidad en sus Normas de Codificación Contable después del 5 de abril de 2012.

Marque en el recuadro que corresponda la base contable que utilizó la entidad registrante para preparar los estados financieros incluidos en esta declaración:

U.S. GAAP | Normas Internacionales de Información Financiera (NIIF) dictadas por el Consejo de Normas Internacionales de Contabilidad ☒ | Otra

Si ha marcado "Otra" en su respuesta a la pregunta anterior, marque en el recuadro que corresponda qué ítem de estados financieros ha elegido seguir la entidad registrante. Ítem 17 Ítem 18

Si el presente constituye un informe anual, marque en el recuadro que corresponda si el registrante es una sociedad instrumental (según la definición contenida en la Regla 12b-2 de la Ley de Bolsas). Sí ☒ No

Indique el número de acciones circulantes de cada clase de acciones de capital social o acciones ordinarias del emisor durante el período cubierto por este informe anual

Acciones Ordinarias

ANEXO 2. CHECK LIST

BUENAS PRÁCTICAS EN EL ÁREA DE TI

NOMBRE DEL EMPRESA: _____

N°	*Fecha de Revisión*	*Detalle*	*Situación*		*Firma Supervisor*	*Observación de situación*		*Observación Superada*	
			SI	*NO*				*Fecha*	*Firma*
Políticas de seguridad de la información									
1		*Establecer e implementar una política de copias de seguridad periódicas.*							
2		*Establecer una política de contraseñas que incluya uso de mayúsculas, minúsculas, números y caracteres especiales.*							
Gestión de activos									
3		*Implementar medidas para la protección física de las copias de seguridad.*							
4		*Realizar pruebas periódicas de restauración de las copias de Seguridad.*							
5		*Implementar controles técnicos para el cambio periódico de las contraseñas de todos los usuarios.*							
6		*Mantener los sistemas y equipos de usuarios actualizados y comprobarlo periódicamente.*							
7		*Realizar auditorías periódicas de seguridad de los servidores.*							
8		*Suscribirse a servicios de noticias de seguridad.*							
9		*Inventariar los activos de TI.*							
10		*Desarrollar procedimientos de las principales tareas técnicas.*							
Control de acceso									
11		*Controlar los permisos de acceso de los usuarios y otorgarlos únicamente a los recursos que necesitan.*							
12		*Asegurar que se sigue una política de segregación de funciones.*							
13		*Implementar controles de acceso físico a áreas restringidas.*							
Evaluación y control de riesgos									
14		*Desarrollar e implantar un procedimiento de gestión de las incidencias de seguridad.*							
15		*Identificar y analizar las vulnerabilidades que se encuentren en las amenazas frecuentes*							

16		*Identificar los riesgos mas críticos e implementar el tratamiento para el mismo*							
17		*Monitorizar la disponibilidad de los servicios y la capacidad de la infraestructura.*							
18		*Llevar a cabo programas de formación y concienciación a empleados.*							
19		*Hoja de resultados de diagnóstico*							
Criptografía									
20		*Establecer una política de cifrado de información confidencial.*							
Estructura de la Seguridad									
21		*Utilizar herramientas de protección como antivirus, IDS, IPS, etc*							
22		*Manuales de procedimientos de responsabilidades operacionales*							
Adquisición desarrollo y mantenimiento de los sistemas									
23		*Procedimientos que se apliquen durante el ciclo de vida de los aplicativos*							
24		*Poseer una política que determine las responsabilidades del personal que administrara los sistemas o el desarrollo*							
Gestión de incidentes de seguridad de la información									
25		*Se gestiona el diagnostico de los incidentes ocurridos*							
26		*Determinar acuerdos de nivel de servicio con proveedores*							
Gestión de la continuidad del negocio									
27		*Desarrollar un plan de recuperación ante desastres.*							
28		*Evaluación de impacto del proyecto*							
29		*Determinar una lista de incidentes que interrumpen las actividades por medio de amenazas*							
30		*Se realizan análisis de impacto de la organización*							
31		*Realizar pruebas Tabletop creando ambiente de crisis*							

_____

Nombre y Firma
Director de TI

ANEXO 3. PASOS PARA DISEÑO DE TABLETOP

	Puntos de la prueba
1	Decidir el nivel de complejidad y daño del evento de interrupción.
2	Calcular el tiempo en que se puede reunir al personal clave para la gestión de la crisis.
3	Involucrar a todos durante la prueba, asignando roles a cada uno de los integrantes.
4	Tener en cuenta que los principiantes en esta clase de pruebas podrían sentirse nerviosos.
5	Sembrar algo de caos ante la situación de prueba, con el fin de simular el estrés y la desinformación ante la crisis.
6	Anotar, confirmar y desplegar las lecciones aprendidas; así como los planes de acción para las mejoras de los planes de contingencia.