MODELO PARA POLITICAS ISO 27001:2013

TABLA DE CONTENIDO

1 INTRODUCCIÓN

La Compañía XXX (la entidad para la que este modelo será usado) se propone implementar un esquema de seguridad de la información, el cual permita asegurar constante y efectivamente la confidencialidad, confiabilidad, eficiencia, el cumplimiento, la integridad y la disponibilidad sobre sus activos de información, siguiendo los lineamientos propuestos por el estándar ISO 27001:2013. Para ello, se requiere que todo el personal que forma parte de la organización conozca, participe y cumpla las **políticas, procedimientos, estándares**, recomendaciones y demás directivas estipuladas en el futuro Sistema de Gestión de Seguridad de la Información (SGSI: ISO 27001:2013).

Para lograr la mejora en la seguridad de la información, este documento establece los **lineamientos, directrices y deberes** de alto nivel que la organización deberá seguir para proteger adecuadamente sus activos de información de acuerdo a estándares internacionales que han sido probados en grandes e importantes empresas a nivel mundial (ISO 27032:2012, ISO 27005:2018, ISO 31000:2018, ISO 27031:2009, PCI DSS, entre otros).

Ilustración 1. Políticas que deben ayudar a proteger la información.

2 MARCO TEÓRICO

El cuidado de la información posee una importancia fundamental para el funcionamiento correcto y efectivo de una determinada organización y además contribuye para que ellas logren en el corto, mediano y largo plazo la consecución de su misión, objetivos de negocio y mejora su probabilidad de supervivencia en un entorno cada vez más dinámico y lleno de riesgos. El hecho de disponer de una serie de controles para mitigar el riesgo según ISO/IEC 27001:2013 e ISO 27032:2012 ayudan a gestionar y proteger los valiosos activos de información; activos indispensables para la operación y funcionamiento de sus procesos organizacionales.

El marco teórico propio de este documento está estrechamente relacionado con la norma ISO 27001:2013. Esta norma ha sido establecida para ofrecer un modelo para el establecimiento, implementación, operación, seguimiento, revisión y mejora de un sistema de gestión de la seguridad de la información (SGSI:ISO 27001:2013). El diseño y la posterior implementación del SGSI de una organización deben estar basados en necesidades, objetivos, los requisitos de seguridad, los procesos empleados y su tamaño y su estructura.

Por otra parte, esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI. Para que una organización pueda cumplir su misión se requiere gestionar y supervisar una serie de actividades o procesos. Se considera un proceso

cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con mucha frecuencia, el resultado de un proceso constituye directamente la entrada al proceso siguiente.

Se puede decir que el proceso de la seguridad de la información busca proteger, según el activo, la confidencialidad, la integridad y la disponibilidad de la información. Estos tres factores son indispensables para asignarle un determinado valor a un activo para proceder a su futura protección después de un análisis de riesgo:

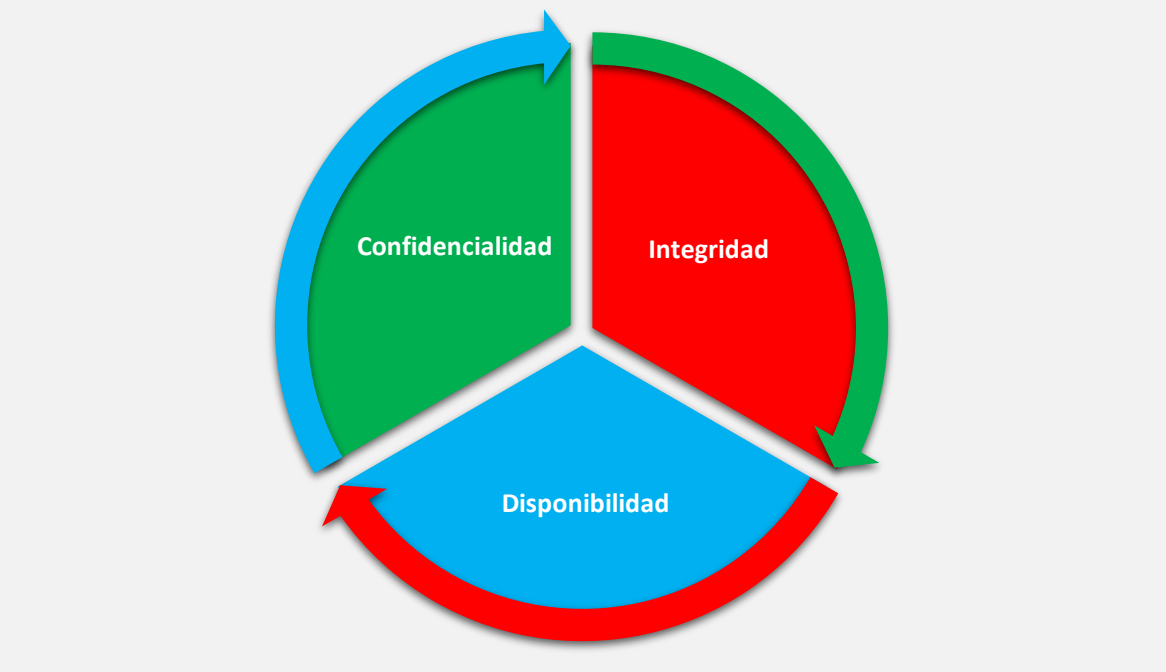

Ilustración 2. Objetivos de la seguridad de la información ISO 27001.

Ahora bien, la adecuada seguridad de la información requiere también considerar los siguientes puntos:

1. Comprender los requisitos de seguridad de la información de la entidad, y la necesidad de establecer políticas de seguridad de la información.
2. Implementar y operar controles para disminuir el riesgo de pérdida de la confidencialidad, integridad y disponibilidad de la información.
3. Medir el desempeño y la eficacia del SGSI ISO 27001.
4. Mantener una mejora continua basada en la medición de objetivos.

Algunos de los conceptos más importantes para implementar la seguridad de la información en los sistemas y componentes serán expuestos a continuación:

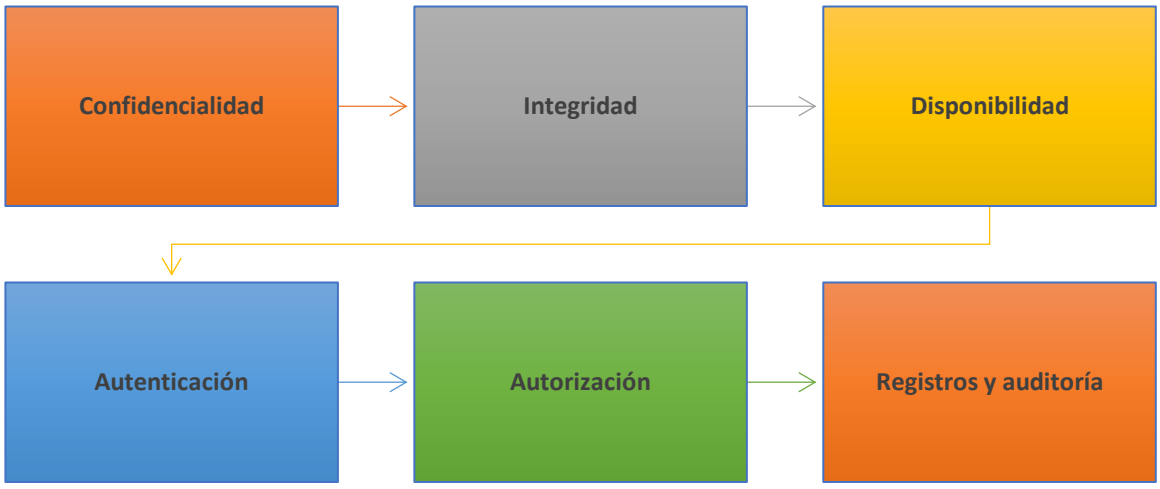

Ilustración 3. Seguridad de la información según ISO 27001.

DISPONIBILIDAD:

Propiedad que determina que la información sea accesible y utilizable por solicitud de una entidad autorizada. La disponibilidad de la información se debe garantizar por medio de los planes de continuidad del negocio o planes para la recuperación ante desastres. Se debe poder acceder a las aplicaciones y a la información que las aplicaciones y sistemas manejan cuando sea requerido y se cuente con la respectiva autorización.

Los acuerdos de servicio (Service level Agreement-SLA) es uno de los ejemplos que pueden citarse para estipular los requerimientos para los sistemas o componentes que soportan los servicios de una determinada organización. El balanceo de cargas y la replicación de información crítica es otro de los dos mecanismos que ayudan a mejorar la disponibilidad de la información.

CONFIDENCIALIDAD:

Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. La confidencialidad protege contra posibles ataques en que la información pueda ser sometida al escrutinio público. Hoy en día muchos ataques tienen en mente el robo de información, por ejemplo, en el caso de la información que está en las tarjetas de crédito que pueden ser fácilmente utilizada para generar robo de dinero y de ahí el interés y el creciente aumento de estos eventos.

INTEGRIDAD:

Propiedad de salvaguardar la exactitud y estado completo de los activos. Se considera que una aplicación o componente posee resiliencia si cumple el papel de proteger la información contra alteraciones de datos no autorizadas. Cuando se realiza una operación financiera uno esperaría que la cantidad de dinero transferido sea igual a la cantidad de dinero que es descontada de la cuenta. En otras palabras, esperamos que las aplicaciones o sistemas sean consistentes en el uso de información. Se requiere que la información que sea transmitida, procesada y almacenada se mantenga consistente según la intención del que realiza la transacción.

AUTENTICACIÓN:

Las aplicaciones, componentes o sistemas en la gran mayoría de organizaciones procesan información sensible, por esta razón es importante que su acceso esté debidamente controlado y solamente aquellas personas o entidades estén debidamente autorizadas. La autenticación responde a la pregunta sobre si lo que se dice ser es verdadero. En otras palabras, durante el proceso de autenticación se realiza una validación de la identidad de la entidad o sistema que solicita el acceso. La autenticación cubre tres aspectos:

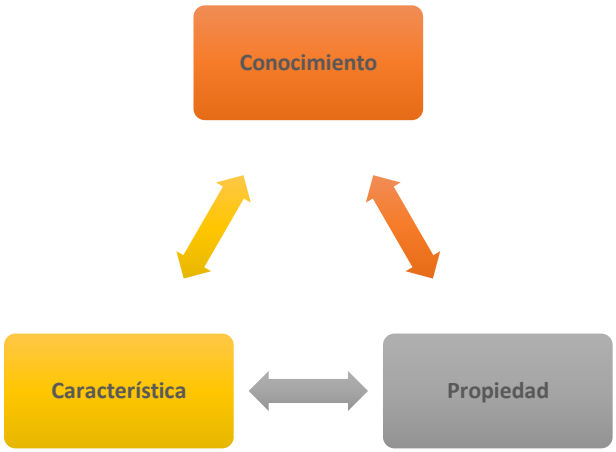

Ilustración 4. Características consideradas en el proceso de autenticación.

Conocimiento: En este aspecto de los tres considerados durante el proceso de autenticación se busca validar solicitando un conocimiento que este usuario, si es quien dice ser, debería poseer. Ejemplos de este tipo de conocimiento están los nombres de usuario, las contraseñas y los números de identificación personal (PIN).

Propiedad: El proceso de identificación en este aspecto se surte por medio de la presentación ante el sistema que identifica de algo que nosotros poseemos y en teoría nadie más posee. Ejemplos de este tipo autenticación son los *tokens* o *smart cards*.

Características: La identificación de la información provista en este aspecto o mecanismo es algo que uno es de manera intrínseca. El ejemplo más difundido es el uso de biométricos. El caso de la huella del dedo y el iris del ojo son características que pueden ser utilizadas para la identificación individualizada.

AUTORIZACIÓN: Por el hecho de que las credenciales de identidad hayan sido validadas no quiere decir esto que se le daba dar acceso a todos los recursos que se soliciten. Por ejemplo, puede darse el caso que a alguien se le pueda dar acceso al software de contabilidad, no obstante, es posible que el acceso a los datos de salarios deba ser bloqueados a él por su nivel de confidencialidad. La autorización es el concepto dentro de la seguridad de la información en que los accesos a los diferentes objetos son controlados y está basado en los derechos y privilegios que son otorgados a los usuarios de acuerdo a las políticas y a los dueños de la información.

REGISTRO Y AUDITORÍA: La creación de registros de los diferentes componentes es importante para que en caso de un incidente de seguridad se pueda contar con la información respectiva que permita realizar la investigación de todos los eventos sucedidos.

A continuación, expondremos los conceptos de seguridad que deben ser considerados cuando se trate de diseñar la arquitectura de un sistema seguro:

Ilustración 5. Objetivos de la seguridad de la información ISO 27001.

MENOR PRIVILEGIO: Un principio dentro de la seguridad de la información en que a un proceso o usuario se le es dado solamente el nivel mínimo de derechos de acceso que son necesarios para que completen una determinada actividad u operación. Este derecho o permiso debe ser concedido solamente por el tiempo requerido para realizar esta actividad.

SEPARACIÓN DE TAREAS: Conocido también como el principio de compartimentación o separación de privilegios, es un principio de seguridad que establece que para realizar una determinada tarea requiere de dos o más condiciones que deben cumplirse sin lo cual no se podría realizar esta tarea.

DEFENSA EN PROFUNDIDAD: También conocido como defensa por niveles, este es un principio de seguridad en donde el compromiso de alguno de los niveles de la defensa no implica que otros niveles sean susceptibles de ataque.

FALLA SEGURA: Este principio de seguridad tiene como objetivos preservar la confidencialidad, integridad y disponibilidad de la información durante una falla del software, de tal manera que el estado en el que se estabilice, estos pilares de la seguridad de la información, sean mantenidos.

ECONOMÍA DE MECANISMOS: A este principio de seguridad subyace la concepción que entre más simple sea el diseño de un componente o sistema la probabilidad de contar con vulnerabilidades potenciales decrece en proporción a esta simplicidad. Si se mantiene el diseño del software dentro de un nivel de simplicidad razonable, la superficie de ataque será reducida.

MEDIACIÓN COMPLETA: Este principio de seguridad establece que cuando un determinado sujeto requiera acceder a un objeto este evento debe ser autorizado y en algunos casos supervisado. Todo acceso siempre debe ser mediado (autorizado) cada vez que se solicite este recurso, es decir, no debe haber excepciones dentro de la gestión del control de acceso.

DISEÑO ABIERTO: En este principio de seguridad para el desarrollo de software se trata de independizar el diseño del software de las técnicas de seguridad que se encuentran implementadas para su defensa, de tal manera que si por alguna razón se hiciera una revisión del diseño general del software las estrategias de seguridad no deben ser comprometidas.

MECANISMOS MÍNIMOS COMUNES: Se evita con este principio que se compartan mecanismos que son comunes a uno o más usuarios o procesos si el usuario y el proceso poseen diferentes niveles de privilegios.

ACEPTABILIDAD PSICOLÓGICA: En este principio se busca que las funciones de seguridad que se implementen en el software sean de fácil uso y lo más transparentemente posible para el usuario final.

ENLACE DÉBIL: Se propone con este principio que la seguridad de un sistema es tan fuerte como su punto más débil. Sea este elemento el código, una interface o servicio.

IGUALANDO LOS COMPONENTES: En este principio se estipula que la superficie de ataque no se incrementa y nuevas vulnerabilidades no son introducidas por el hecho de promover la reutilización de componentes del software, código y funcionalidad.

3 NORMAS APLICABLES

- NTC/ISO 27001:2013
- NTC/ISO 27005:2018
- ISO 31000:2018
- ISO 27032:2012
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL

4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de la Seguridad de la Información basado en ISO 27001:2013 es soportado por las políticas de seguridad de la información y tiene las fases de Planear, Hacer, Verificar y Actuar:

Ilustración 6. Ciclo PHVA.

5 OBJETIVOS DE LAS POLÍTICAS

El propósito de las Políticas de Seguridad de la Información basadas en ISO 27001:2013 es proteger los activos de información de todas las amenazas internas o externas, bien sean intencionales, naturales o accidentales.

Debe ser política de la organización asegurar la:

- **Confidencialidad** de la información, de manera que únicamente usuarios autorizados tengan acceso.
- **Integridad** de la información, evitando su alteración no autorizada.
- **Disponibilidad** de la información, asegurando su presencia cuando sea requerida por usuarios debidamente autorizados y en un tiempo razonable de respuesta.
- **Cumplimiento** de las leyes y regulaciones.
- **Entrenamiento** a todos los empleados en el tema de seguridad de la información.

6 ROLES Y RESPONSABILIDADES

Estas políticas basadas en ISO 27001:2013 deben ser aprobadas por las directivas luego de un estudio previo y detallado de sus posibles consecuencias con el fin de lograr la continuidad y la seguridad en la operación del negocio. Estas políticas también son de obligatorio cumplimiento para todos los empleados, contratistas y terceras partes.

7 VIOLACIONES A LA POLÍTICA

Las violaciones a las políticas deberán conducir a procesos disciplinarios de acuerdo a la legislación colombiana y en conjunto con lo definido por el departamento de recursos humanos.

8 REVISIÓN DE LA POLÍTICA

Estas políticas deben ser modificadas si existiesen cambios importantes en los procesos de negocio de XXX o en su infraestructura tecnológica, de no haber cambios, se debe realizar su revisión anualmente.

9 TÉRMINOS Y DEFINICIONES UTILIZADOS EN ESTE DOCUMENTO

Activos de información: Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio y de soporte. Se pueden clasificar de la siguiente manera:

- **Personas:** Incluyendo sus calificaciones, competencias y experiencia.
- **Intangibles:** Ideas, conocimiento, conversaciones.
- **Electrónicos**: Bases de datos, archivos, registros de auditoría, aplicaciones, herramientas de desarrollo y utilidades.
- **Físicos**: Documentos impresos, manuscritos y hardware.
- **Servicios**: Servicios computacionales y de comunicaciones.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Política de Seguridad: Una política de seguridad, es una declaración formal de las reglas, directivas y prácticas que rigen la forma de gestión de los activos de tecnología e información dentro de una organización.

Procedimientos: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Estándares: Un estándar es definido como un producto o mecanismo especifico el cual es seleccionado desde un punto de vista universal, para su uso a lo largo de toda la organización, con el objetivo fundamental de soportar una política ya aceptada y aprobada por las directivas de la compañía.

Comité de seguridad: Su función principal es garantizar que exista una clara dirección y un soporte adecuado para las iniciativas de seguridad, junto con el hecho de poder promover la cultura de seguridad a través de toda la organización, obteniendo de la misma manera los recursos disponibles para ello y está conformado por un grupo interdisciplinario.

Área IT: Es el área encargada de soportar, diseñar y mantener los activos electrónicos y el hardware. Tambien se conoce como departamento de sistemas. Es recomendable que el esta área este soportada por la gerencia general. Otras áreas también podrían líder el proceso de seguridad de la información.

Terceros: Entendemos por terceros a proveedores, contratistas, clientes y visitantes a XXX.

Contratistas: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con XXX.

Consultor: Persona idónea en capacidad de prestar servicios de asesoría, diseño, y creación de propiedad intelectual.

Información: Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos. Por ejemplo:

- Una noticia que escuchamos por la radio.
- Una señal de tráfico que advierte un peligro.
- Una fórmula que usamos en un problema.

La información se representa mediante conjuntos de símbolos, que pueden ser de diferente naturaleza:

1. Textuales o numéricos, como las letras y números que usamos al escribir.
2. Sonoros, como los fonemas, las notas musicales...
3. Cromáticos, como los colores de los semáforos.
4. Gestuales, como los que usamos para hacer mímica.

Propietario: Es el responsable y dueño del activo de información. Define también sus niveles de clasificación.

Custodio: Encargado de proteger la información por delegación del propietario. Generalmente este rol es ejecutado por el Área de tecnología.

Usuario: Es el que utiliza los activos de información para llevar a cabo las funciones de su trabajo.

Incidente de Seguridad: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una posibilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Red privada virtual – VPN: Método de conexión a través de una red publica o privada, que permite a los usuarios establecer conexiones seguras. La utilización más frecuente corresponde a la conexión por Internet.

Oficial de Seguridad: Persona responsable por velar, mantener y gestionar la seguridad de los activos de información y que cuenta con el apoyo de las directivas y ademásj posee un conocimiento integro de la seguridad de la información.

10DOMINIOS DE ISO 27001:2013

Los dominios de la norma ISO 27001:2013 son los siguientes:

Dominio ISO 27001:2013	Objetivo de control
Política de seguridad.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y ambiental.	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad.	Objetivo de control A.16
Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Política de seguridad: Constituye el presente documento, y es donde se estipulan las políticas con respecto a la seguridad de la información siguiendo los lineamientos dados por ISO 27001:2013.

Organización de la seguridad: Gestionar la seguridad de la información. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros)

Seguridad del Recurso Humano: Este dominio busca asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles a desempeñar minimizando los riesgos relacionados con personal.

Gestión de activos: Se relaciona con el mantenimiento y protección apropiados de todos los activos de información.

Control de acceso: Se realiza el control físico o lógico de los accesos a los activos de la información, incluyendo por ejemplo acceso físico a los sistemas operativos o aplicaciones.

Criptografía: Tecnología para evitar que la información sea divulgada sin autorización.

Seguridad Física y del entorno: Busca prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones y a su información.

Seguridad en las operaciones: Se busca asegurar la correcta y segura operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica).

Seguridad en las comunicaciones: Se busca asegurar la correcta y segura operación de las comunicaciones que posee la organización.

Adquisición, desarrollo y mantenimiento de sistemas de información: Asegurar la inclusión de todos los controles de seguridad en los sistemas de información nuevos o en funcionamiento (infraestructura, aplicaciones, servicios, etc.). También regula la adquisición de software para la organización y los contratos de soporte y mantenimiento asociados a ellos.

Relación con proveedores: Los proveedores son entidades que deben contar con un mínimo de seguridad.

Gestión de incidentes de seguridad: Permitir que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados de tal manera que se tome una acción correctiva adecuada y en el momento indicado.

Gestión de la continuidad del negocio: Enfocado en reaccionar en contra de interrupciones a las actividades de la función misional y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y por otro lado, asegurar que se recuperen a tiempo.

Cumplimiento: Busca prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

11POLÍTICAS POR DOMINIOS

11.1 POLÍTICA DE SEGURIDAD ISO 27001

El objetivo de optar por la definición a un conjunto de políticas en seguridad de la información según el estándar ISO 27001:2013, es brindar apoyo y orientación a la gerencia y a los empleados con respecto a la protección de los activos de información de acuerdo con los requisitos del negocio, los reglamentos y las leyes pertinentes, con el fin de lograr una operación segura y confiable de la organización.

La gerencia o dirección general debe aprobar, publicar, comunicar a todos los empleados o partes externas pertinentes el documento de políticas de seguridad de la información según ISO 27001:2013. Para ello se sugiere entre otras actividades las siguientes:

1. carpetas publicas con su debida protección
2. Envío de correo electrónico referenciando su ubicación
3. Plan de entrenamiento para su divulgación
4. Ubicación física pública

Las políticas y normas de seguridad de la información expresadas en este documento, se deben revisar una vez al año o cuando se produzcan cambios significativos en los procesos, la infraestructura, el software, las aplicaciones y todo aspecto que influya considerablemente en la organización, con el fin de asegurar que ella, siga estando operativa y cumpla con su misión en el transcurso del tiempo. Esta revisión será realizada por el **oficial de seguridad** y aprobada por el **comité de seguridad**.

11.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

11.2.1 Organización Interna

En este dominio se definen las directrices para gestionar y establecer las responsabilidades con respecto a la seguridad de la información de acuerdo a la norma ISO 27001:2013.

11.2.2 Compromiso de la gerencia con la Seguridad de la Información

La gerencia o dirección general debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y con el establecimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

- La creación de un comité de seguridad interdisciplinario
- La asignación de un responsable de la seguridad de la información(Oficial de seguridad)
- La aprobación formal del documento de políticas de seguridad de la información
- La asignación de responsabilidades asociadas al tema de la seguridad de la información
- Y el ejemplo en el cumplimiento de las normas

11.2.3 Funciones del Comité de Seguridad de la información

El comité de seguridad de la información debe estar conformado por miembros de alto nivel de los departamentos y áreas de la organización:

- Debe periódicamente revisar el estado general de la seguridad de la información
- Revisar informe ejecutivo de incidentes de seguridad de la información
- Revisar y aprobar los proyectos de seguridad de la información
- Aprobar las modificaciones o nuevas políticas de seguridad de la información
- Realizar otras actividades de alto nivel relacionadas con la seguridad de la información

Por último, cuando el comité de seguridad se reúna con el propósito de revisar temas de seguridad de la información se incluirá la participación del Oficial de Seguridad.

11.2.4 Coordinación de la Seguridad de la Información

Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes con roles y funciones laborales pertinentes.

1. La gerencia o dirección será responsable de que los empleados a su cargo, conozcan y apliquen las políticas de seguridad de la información.

2. Se deberá contar con un Oficial de Seguridad de la Información que asuma las tareas y responsabilidades que conlleva este rol:

    a. Definir y actualizar políticas, normas, procedimientos y estándares definidos en el SGSI ISO 27001.
    b. Validar la arquitectura de seguridad en todos los ambientes (desarrollo, pruebas, producción y contingencia)
    c. Realizar el análisis de riesgo a las aplicaciones
    d. Revisar, documentar y aprender de los incidentes de seguridad
    e. Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio
    f. Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información
    g. Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios
    h. Promover la formación, educación y el entrenamiento en seguridad de la información
    i. Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes

j. Recibir capacitación en el tema de seguridad de la información
k. Realizar estudios de penetración y pruebas de seguridad en todos los ambientes[1] (Desarrollo, Pruebas, Producción y Contingencia)

11.2.5 Asignación de responsabilidades para la Seguridad de la Información

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información. En especial las relacionadas a la existencia de un comité de seguridad y un oficial de seguridad.

11.2.6 Oficial de Seguridad

Se debe contar dentro de la planta de empleados un Oficial de Seguridad de la información.

11.2.7 Comité de seguridad

El Oficial de Seguridad podrá convocar a diferentes empleados para formar grupos interdisciplinarios que apoyen la definición e implementación de los diferentes temas de seguridad de la información.

11.2.8 Dueños de la Información

Toda la información utilizada por la organización debe poseer un dueño. Estos dueños de la información son responsables de estos activos y deben:

- Definir la clasificación de la información(pública, interna o privada)
- Determinar los niveles de acceso a la información
- Autorizar la asignación de permisos de acceso
- Apoyar en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información

11.2.9 La gerencia

La gerencia es responsable que los empleados a su cargo, conozcan y apliquen las políticas de seguridad de la información.

11.2.10 Empleados

Son responsables por el cumplimiento de las políticas de seguridad de la información. Adicionalmente cada empleado está obligado a reportar al Oficial de Seguridad cualquier incidente de seguridad del que tenga conocimiento.

11.2.11 Contratistas, proveedores y terceros

Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir las políticas de Seguridad de la Información.

11.2.12 Administradores de los sistemas

Los administradores de los diferentes sistemas deben en forma activa implementar las normas, estándares, formatos y procedimientos, para brindar un nivel apropiado de seguridad de la información.

11.2.13 Autorización para nuevos servicios de procesamiento de la Información

Se debe definir e implementar un procedimiento de autorización de la gerencia para nuevos servicios de procesamiento de la información.

Se debe considerar para esta implementación los siguientes aspectos:

1. La asignación de un dueño para cualquier nuevo servicio a implementar, además incluyendo la definición de las características de la información, tales como clasificación y definición de los diferentes niveles de acceso por usuario.
2. El dueño de la información debe explícitamente dar autorización para usar este nuevo servicio.

[1] Para esta actividad se recomienda el uso de la herramientas LanGuard de GFI.

3. Se debe contar con la autorización respectiva por parte del oficial de seguridad de la información, garantizando que el nuevo servicio cumple con las políticas de seguridad de la información definidas en este documento.
4. Evaluar la compatibilidad a nivel de hardware y software con otros sistemas.
5. Identificar las vulnerabilidades que genere el nuevo servicio y además definir los controles necesarios para mitigarlas.

Además de los puntos anteriores los pasos para la adquisición de un nuevo servicio ya sea de transporte, almacenamiento o procesamiento de la información, deben seguir las siguientes actividades cuando el valor del activo exceda X cantidad de dinero:

1. Estudio de la necesidad
2. Se debe hacer una investigación del estado del arte en el activo de información que se va a adquirir, y seleccionar tres (3) fabricantes que cumplan con las especificaciones técnicas. También se requiere que el elemento a adquirir cumpla estándares de seguridad y permita realizar configuraciones para mejorar la protección de la información de acuerdo a recomendaciones internacionales como ISO 27001:2013, CMM[2], COBIT 5.0, ITIL V.3, ICSA y otros (ver recomendaciones para adquisición de software en ISO 27001:2013 y PCI DSS). Lo anterior nos debe generar como salida un *documento de especificaciones técnicas* (RFP[3]).
3. Se debe generar una orden de trabajo.
4. Se debe contar con autorización del Jefe de Departamento.

11.2.14 Acuerdos de confidencialidad

Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades para la protección de la información.

Todos los empleados, contratistas, proveedores y terceros, que deban realizar labores dentro de la organización, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información, para empleados y terceros.

11.2.15 Contactos con las autoridades

El oficial de seguridad de la información debe identificar los organismos externos que ejerzan autoridad en lo relacionado con los aspectos de seguridad de la información y definir el mecanismo para su contacto. Los contactos con las autoridades incluyen servicios públicos, servicios de emergencia, salud, organismos de regulación y control entre otros

11.2.16 Contactos con grupos de interés

El oficial de seguridad de la información debe de forma permanente identificar comunidades y grupos de interés relacionados con la Seguridad de la Información y establecer contacto con ellos con el fin de estar actualizado en estos temas. Entre ellos se pueden recomendar los siguientes:

- CERT(www.cert.org)
- SANS(www.sans.org)
- ISC(www.isc2.org)
- ISACA(www.isaca.org)

11.2.17 Revisión independiente de la Seguridad de la Información.

Las políticas de seguridad de la información, normas, controles, estándares, formatos y procedimientos, deben ser revisados periódica y planificadamente, por un área independiente de sistemas dentro de XXX o por un organismo o consultor externo. Este periodo debe ser de al menos *una vez al año* o cada vez que ocurra un cambio sustancial en la infraestructura o activos de información de la organización. La auditoría requerida

[2] Capability Maturity Model.
[3] Request For Proposal (Requerimiento para una propuesta)

seguirá los linimientos ISO 27001:2013, realizada por alguien con las credenciales de AUDITOR LIDER (Lead Auditor) 27001:2013 vigentes.

11.3 GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

11.3.1 Responsabilidad por los activos

El objetivo de este dominio es la protección adecuada de los activos de la información propiedad de la organización en cuestión.

11.3.2 Inventario de Activos

Se deben mantener todos los activos de información claramente identificados, referenciados. La organización debe identificar todos los activos y documentar su importancia. El inventario de activos debe incluir toda la información necesaria para recuperarse de los desastres, incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y su valor.

Tipos de activos:

- Información
- Activos de software
- Activos físicos
- Servicios
- Personas y sus calificaciones
- Intangibles
- Aplicaciones
- Servidores

11.3.3 Propiedad de los activos

Toda la información y los activos asociados con los servicios de procesamiento, almacenamiento y transferencia de información deben ser propiedad[4] de la parte designada.

El propietario del activo deberá ser responsable de:

- Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente
- Velar por la protección de la información
- Definir sus activos críticos de la información
- Definir y revisar periódicamente (una vez al año) las restricciones y niveles de acceso, teniendo en cuenta las políticas aplicables sobre el control de acceso.

Por otro lado, la propiedad se puede asignar a:

- Un proceso de negocio
- Un conjunto definido de actividades
- Una aplicación
- Un conjunto definido de datos

Una vez al año se debe efectuar una revisión detallada de los inventarios de los activos de la información, con el objetivo de tener un control directo sobre el estado y situación de estos activos, de acuerdo con las políticas de seguridad de la información, para asegurar su adecuada protección en términos de disponibilidad y confidencialidad.

El alcance de esta política considera los siguientes tipos de activos:

[4] El término propiedad identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término propietario no implica que la persona tenga realmente los derechos de propiedad de los activos.

- Software
- Físicos
- Servicios
- Personales
- Intangibles

11.3.4 Uso aceptable de los activos

Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información. El mantener escritorios limpios y debidamente aseguradas las estaciones de trabajo es parte integral de esta política.

11.3.5 Escritorios libres en horas no laborales

Por fuera del horario regular de trabajo, todos los empleados deben mantener sus escritorios y áreas de trabajo libres de cualquier información considerada sensitiva, confidencial o crítica, además deben asegurar en forma apropiada esta información utilizando controles ya sean físicos o lógicos antes de salir de la organización.

11.3.6 Escritorios libres en horas habituales de trabajo

A menos que la información se esté utilizando por personal autorizado, los escritorios deben estar absolutamente libres durante horas laborales y toda la información considera como confidencial debe estar asegurada en forma adecuada.

11.3.7 Manejo de Información en horario laboral

La información considerada como sensitiva, confidencial o crítica debe siempre permanecer bajo llave en los archivadores destinados para tal fin.

11.3.8 Áreas Desatendidas

Mientras no se encuentre en uso, la información sensitiva que resida en áreas desatendidas, o sin vigilancia, debe ser asegurada en forma apropiada por medio del uso de controles de acceso físico o lógicos según sea el caso.

11.3.9 Almacenamiento de Información sensitiva o confidencial

Toda la información impresa o en medios de almacenamiento considerada como confidencial, o importante para el funcionamiento de los sistemas de información, debe ser asegurada en forma adecuada, utilizando para esto archivadores con llave, cajas fuertes y sistemas de protección contra acceso físico. Las llaves deben estar en un sitio desconocido para todo aquel que no sea su administrador y también deben poseer un medio de control de acceso físico.

11.3.10 Apagado y bloqueo de Estaciones de Trabajo

Todas las estaciones de trabajo, deben ser apagadas al final de la jornada laboral. En caso de un retiro momentáneo se debe realizar la función de bloqueo de su estación, para ello en Windows utilizar la función CTRL-ALT-SUP.+ Bloqueo de estación.

11.4 SEGURIDAD DEL RECURSO HUMANO

11.4.1 Antes de la contratación laboral

Este dominio busca asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y además sean los adecuados para los roles a desempeñar logrando de esta manera reducir el riesgo de robo, fraude o uso no adecuado de las instalaciones.

11.4.2 Roles y responsabilidades

Todos los empleados nuevos que hayan aprobado los procesos de selección, deberán conocer, entender y asumir las responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar. Igualmente es responsabilidad de todo empleado vinculado con anterioridad a la elaboración de este documento, conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar. Estos roles y responsabilidades de los empleados, contratistas y terceros deben estar debidamente documentados.

11.4.3 Selección

Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser próximos empleados, contratistas o terceros, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y a los riesgos percibidos.

11.4.4 Términos laborales

Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades con relación a la seguridad de la información.

11.4.5 Durante la vigencia de la contratación laboral

El objetivo es asegurar que todos los empleados, contratistas o terceras partes estén conscientes de las amenazas respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

11.4.6 Responsabilidades de la gerencia

La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes, apliquen la seguridad según las políticas y los procedimientos establecidos.

11.4.7 Entrenamiento, educación y formación

Se debe entrenar, educar y formar a los empleados, contratistas, proveedores y terceros en los temas de seguridad de la información, necesarios para asegurar que no se infrinja el esquema de seguridad debido a falta de capacitación o desconocimiento del SGSI.

Es importante desarrollar un programa de formación y cultura, con el fin de educar a todos los empleados de la organización. Los empleados deben entender y respetar las buenas prácticas de seguridad de la información.

Se debe manter un proceso continuo de evaluación sobre la efectividad de la formación proporcionada y de los planes de mejoramiento que de él se deriven. Esta evaluación se deberá realizar una vez cada año para todo empleado en un sistema que estará presente dentro de la organización.

Conciencia de la seguridad: Durante esta fase, los empleados adquieren conocimiento sobre los temas que deben tener presentes en el área de seguridad de la información, los esquemas mínimos a considerar y las mejores prácticas existentes en seguridad. Esta fase constituye el acercamiento inicial al modelo de seguridad y su duración no debe exceder los seis (6) meses; tiempo durante el cual se darán charlas, se publicarán avisos e información relevante en diferentes tipos de formatos para su lectura, entendimiento y comprensión. Una vez terminado este proceso, es necesario dar continuidad a la conciencia en seguridad.

Formación: En esta fase se entrena a los empleados a responder de forma adecuada ante incidentes de seguridad de la información que se presenten en los activos de información. Se busca que los empleados conozcan la respuesta adecuada ante incidentes, creando así una conducta que pueda ser repetida y se convierta con el tiempo en un patrón de actuación.

Educación: En la última fase del proceso, se completa el ciclo inculcando en los empleados el porqué de la seguridad de la información y de todo el sistema, se profundiza en temas específicos, se dan las pautas y entrenamientos a los empleados que lo requieran en especializarse en ciertos campos de la seguridad, además, se proponen espacios de debate con el fin de plantear esquemas más avanzados de seguridad que aporten buenas prácticas. Se recomienda entrar en procesos de certificación[5] internacional en seguridad de la información a través de entidades como ISACA e ISC[2], que soportan las certificaciones CISA, CISM y CISSP respectivamente.

11.4.8 Proceso disciplinario

El incumplimiento de alguna de las políticas o regulaciones estipuladas en el SGSI que conlleve a un incidente de seguridad, implicará un proceso disciplinario, el cual previamente ha establecido las responsabilidades del empleado involucrado.

11.4.9 Terminación o cambio de la contratación laboral

El objetivo de esta política es asegurar que los empleados, contratistas o terceras partes se retiren de la organización o cambien su contrato laboral de forma ordenada.

11.4.10 Responsabilidades en la terminación

Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.

11.4.11 Devolución de activos

Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo. La cuenta de este usuario debe ser bloqueada inmediatamente y sus retiro se hará en los próximos dos (2) días hábiles.

11.4.12 Retiro de los derechos de acceso

Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio. El jefe de departamento o gerente de planta, debe diligenciar oportunamente el formato respectivo. La cuenta de este usuario debe ser bloqueada inmediatamente y su retiro se hará en los próximos tres (3) días hábiles.

[5] Para mayor información consultar www.isaca.org y www.isc2.org.

11.5 SEGURIDAD FÍSICA Y AMBIENTAL

11.5.1 Áreas seguras

Esta política evita el acceso no autorizado, el daño e interferencia a las instalaciones y a la información.

11.5.2 Perímetro de seguridad física

Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas y otros) para proteger las áreas que contienen información y servicios de procesamiento de información.

- Todos los terceros que requieran ingresar a las instalaciones deberán estar adecuadamente identificados y anunciar su llegada a través del personal de vigilancia de las instalaciones, con el fin de obtener la respectiva autorización. Entre los activos a considerar tenemos:
    - Portátiles
    - Memorias USB
    - Cámaras fotográficas
    - Smartphones
    - Celulares con puertos USB o cámaras fotográficas o de video
- Las puertas de acceso a las áreas de manipulación o administración de información confidencial o privada, deberán permanecer cerradas y bajo llave en todo momento para que no exista nadie autorizado haciendo uso de ellas.

11.5.3 Controles de seguridad física

Todas las personas que ingresen a las áreas restringidas de la organización, deberán cumplir con los controles establecidos para el acceso específico a dichas áreas. Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

11.5.4 Seguridad de oficinas, recintos e instalaciones

Se debe diseñar y aplicar las políticas de seguridad física para oficinas, recintos e instalaciones.

11.5.5 Protección contra amenazas externas y ambientales

Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundaciones, terremoto, explosión, manifestaciones sociales y otras formas de amenazas natural.

Se deben mantener las condiciones físicas y ambientales óptimas recomendadas para centros de cómputo así como controles automáticos para prevenir incendios y aumentos de temperatura. A continuación una serie de recomendaciones y normas a considerar en el centro de cómputo:

- Fallas en el control de la temperatura o humedad pueden afectar la operación del negocio, así que, se debe tener un estricto monitoreo sobre estas variables.
- En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio.
- Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Se deben tener extintores de incendios debidamente probados, y con capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- Inundación o falta de suministro
- Las salas de procesamiento de la información deberán estar ubicadas de ser posible en pisos a una altura superior al nivel de la calle a fin de evitar inundaciones.
- Las cañerías de desagüe de dichas salas y ubicadas en el piso, deberán poseer válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación ante sobre-flujos.

11.5.6 Trabajo en áreas seguras

Se debe diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

11.5.7 Áreas de carga, despacho y acceso público

Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y si es posible, aislar de los servicios de procesamiento de información para evitar acceso no autorizado.

11.5.8 Seguridad de los equipos

El objetivo de esta política es evitar pérdida, daño, robo o puesta en peligro de los activos y la posible interrupción de las actividades.

11.5.9 Ubicación y protección de los equipos

Los equipos pertenecientes a la organización deben estar ubicados o protegidos para reducir el riesgo debido a amenaza o peligros del entorno, y las posibles oportunidades de acceso no autorizado.

11.5.10 Almacenamiento de cintas de respaldo

Se contará con un sitio adecuado y asegurado para la custodia de la información que se encuentra en cintas. Se considera a este sitio como parte funcional del centro de cómputo a pesar de que por seguridad se trata de un recinto contiguo pero independiente.

11.5.11 Servicios de suministros

Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro. Se debe contar con un sistema de UPS y un generador de energía en caso de fallas prolongadas de potencia.

- El correcto uso de UPS (Uninterruptable Power Suply), las cuales se deben probar según las recomendaciones del fabricante, de tal forma que garanticen el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.
- El Generador debe ser regularmente probado de acuerdo a las recomendaciones del fabricante, o por lo menos una vez al año.
- Se deben tener interruptores eléctricos adicionales, localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en caso de una falla o contingencia. Las luces de emergencia deben funcionar en caso de fallas en la potencia eléctrica.

11.5.12 Seguridad del cableado

El cableado que incluye tanto el de energía eléctrica como el de comunicaciones, el cual transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones. Los *racks* deben estar bajo llave en los diferentes pisos o sectores. Las llaves a su vez deben estar protegidas por un sistema de acceso físico y procedimientos respectivos.

11.5.13 Mantenimiento de los equipos

Se establecerán esquemas de mantenimiento para toda la plataforma tecnológica que deberán ser cumplidos dentro de las fechas programadas. Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad de acuerdo a las especificaciones dadas por el fabricante.

Al disponer de un disco duro utilizado, ya sea para su entrega, reutilización o asignación, deberá pasar por un proceso adecuado de borrado seguro.

11.5.14 Seguridad de los equipos fuera de las instalaciones

También es importante considerar el hecho de poder suministrar seguridad a estos equipos cuando sean requeridos o utilizados fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar en estas condiciones.

- La información confidencial no debe salir nunca del perímetro de la organización sin la respectiva autorización del dueño de la misma.
- Si un portátil, computador o smartphone debe salir por alguna razón y con su respectiva autorización, se deben tomar las siguientes medidas de seguridad:

    - Debidamente protegido en un maletín, en lo posible que no sea de color negro
    - La información confidencial debe estar cifrada con los mecanismos que para ello ofrece el sistema operativo (Bitlocker o TDE)
    - El equipo no debe nunca ser desatendido en aeropuertos, restaurantes o hoteles

11.5.15 Seguridad en la reutilización o eliminación de equipos

Se deben verificar todos los elementos de los equipos que contengan medios de almacenamiento en caso de reutilización o eliminación para asegurar que se haya borrado cualquier software licenciado o datos sensibles y además se debe comprobar que se hayan sobrescrito de forma confiable antes de la eliminación.

Cuando un medio magnético propiedad de la organización termine su ciclo de vida, deberá ser destruido de acuerdo a las exigencias propuestas. Al disponer de un disco duro utilizado, ya sea para su entrega, reutilización o eliminación, deberá pasar por un proceso adecuado de borrado seguro.

11.5.16 Retiro de activos

Ningún equipo, sistema o computador se debe retirar sin la respectiva autorización.

11.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

11.6.1 Procedimientos operacionales y responsabilidades

El objetivo de este dominio es asegurar la operación correcta y segura de los servicios de procesamiento, almacenamiento y transporte de la información.

11.6.2 Documentación de los procedimientos operativos

Todos los procedimientos operativos considerados críticos estarán adecuadamente documentados, mantenidos y a disposición de los operadores a quienes compete. Es responsabilidad de la organización mantener debidamente actualizada toda la documentación referente a la plataforma tecnológica.

11.6.3 Gestión del Cambio

Cualquier cambio a la plataforma tecnológica deberá ser completamente documentado, revisado, aprobado, y controlado. Cualquier cambio realizado a las aplicaciones desarrolladas para la operación normal, deberá ser completamente documentado y sus versiones controladas según los requerimientos establecidos. Todos los cambios en el ambiente de producción deberán ceñirse a las regulaciones establecidas para la adecuada puesta en producción.

11.6.4 Distribución de funciones

Las funciones y las áreas de responsabilidad se deben distribuir con el fin de reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.

11.6.5 Separación de ambientes

Se mantendrán identificados, controlados y aislados los ambientes de Prueba, Desarrollo y Producción, aplicando para cada uno los procedimientos específicamente estipulados.

11.6.6 Planificación y aceptación del sistema

El objetivo de esta política es minimizar el riesgo de fallas de los sistemas en operación.

11.6.7 Gestión de la capacidad

La plataforma tecnológica será continuamente monitoreada con el fin de establecer adecuados niveles de capacidad y desempeño, empleando las herramientas eficaces y manteniendo actualizada la debida documentación.

11.6.8 Aceptación del sistema

Se deben establecer criterios de aceptación para los sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo las pruebas adecuadas del sistema durante el desarrollo y antes de la aceptación y puesta en funcionamiento en producción.

11.6.9 Protección contra código malicioso o móvil

Se busca con esta política proteger la integridad del software y de los activos de información.

11.6.10 Controles contra código Malicioso

Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como programas apropiados para la toma de conciencia de los empleados o funcionarios.

- Se contará permanentemente con un sistema efectivo de antivirus que será administrado bajo la responsabilidad definida, y su configuración debe estar regulada por un estándar de seguridad.
- Los usuarios deberán cumplir con las *mejores prácticas* establecidas con respecto al uso del Antivirus.
- Es responsabilidad de cada funcionario o tercero, revisar que todos los medios magnéticos extraíbles sean chequeados con un antivirus antes de procesarlos en los computadores personales o servidores.

- Se debe mantener en buen funcionamiento los sistemas que le permitan prevenir, detectar y corregir ingresos ó intentos de ingresos no autorizados.

11.6.11 Controles contra códigos móviles

Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida y se debe evitar la ejecución de los códigos móviles no autorizados. Esta función puede habilitarse o deshabilitarse en el Firewall o en el navegador de Internet.

11.6.12 Respaldo

Se debe mantener la integridad y la disponibilidad de la información y de los servicios de procesamiento, almacenamiento y transporte de ella.

11.6.13 Respaldo de la informació

Para el respaldo de la información se debe:

- Toda la información debe ser respaldada por medio de copias de seguridad siguiendo el procedimiento adecuado según el componente. Esto incluye la información de los usuarios, la cual se encuentra en las carpetas del servidor destinadas para esa función. También se debe poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

- Es responsabilidad del dueño de la información, definir los periodos de retención y la frecuencia de los Backups que garanticen la continuidad del negocio y la consulta histórica de su información.

11.6.14 Gestión de la seguridad en las redes

El objetivo de esta política es asegurar la protección de la información en las redes y la respectiva protección de los activos de información.

11.6.15 Controles de las redes

Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en transito. Se implementará la función de listas de control de acceso en la infraestructura de red con el fin de mejorar el control sobre el tráfico que viaja sobre ellas. Además de lo anterior, se deben implementar los siguientes estándares de configuración: “**Estándar de configuración switches**”, “**Estándar de configuración firewall**”.

11.6.16 Seguridad de los servicios de red

En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan localmente o se contratan externamente. Este acuerdo de prestación de servicios debe hacerse con el dueño de la información o el dueño del sistema de información.

- Se mantendrá un constante monitoreo sobre la red interna, implementando las herramientas que le permitan detectar, prevenir y recuperarse contra código malicioso encontrado en su plataforma tecnológica.

- La transmisión externa de datos personales u otra información confidencial de XXX por Internet está estrictamente prohibido.

- El uso de la Internet para cualquier empleado debe ser autorizado, previo diligenciamiento del respectivo formato el cual será suministrado oportunamente.

11.6.17 Manejo de los medios

El objetivo de esta política es evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y una posible interrupción en las actividades.

11.6.18 Procedimiento para el manejo de la información

Se deben establecer procedimientos para el manejo y almacenamiento de la información residente en los medios, con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.

11.6.19 Seguridad de la documentación del sistema

La documentación del sistema debe estar protegida contra el acceso no autorizado. Para ello se deben tener mecanismos de control de acceso físicos y sistemas bajo llave, garantizando la debida protección de estas llaves.

11.6.20 Mensajería electrónica

La información contenida en la mensajera electrónica debe tener la protección adecuada.

- Los usuarios deber ser especialmente cuidadosos con los destinatarios colectivos y los foros de discusión.
- Las leyes de derechos de autor y licencias de software también aplican para el correo electrónico.
- La información de los mensajes del correo electrónico deben ser borrados una vez que la información contenida en ellos ya no sea de utilidad.
- Se debe cifrar la información considerada como confidencial.

11.6.21 Monitoreo

El objetivo de esta política es poder estar en capacidad de detectar actividades de procesamiento de la información no autorizada.

11.6.22 Registro de auditorias

Se realizará un monitoreo permanente de la red y los sistemas a través de los diferentes *logs* establecidos y configurados a conveniencia. Estos *logs* serán revisados, guardados y analizados de acuerdo a las tareas programadas. Esta actividad se realiza con el fin de facilitar futuras investigaciones cuando se presente un incidente de seguridad. Los *logs* se mantendrán por un periodo de dos (1) años y su respaldo se hará cada mes. Es recomendable tener un servidor al cual se envíe los *logs* de los servidores críticos, firewalls y switches de red.

- Logs de servidores serán revisados una vez al día.
- Logs de switch central de la red será revisado una vez al día
- Logs de firewall serán revisados una vez al día.

11.6.23 Monitoreo del uso del sistema

Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información y los resultados de las actividades de monitoreo se deben revisar con regularidad.

11.6.24 Protección de la información de los registros

Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizada. El administrador del sistema no debe estar en capacidad de modificar la información existente en los registros, y a su vez esta información debe contar con un mecanismo de respaldo para garantizar su disponibilidad.

11.6.25 Registros del administrador y operador

Se deben registrar las actividades tanto del operador como del administrador del sistema. Se debe tener especial cuidado con los usuarios privilegiados.

11.6.26 Registros de falla

Las fallas se deben registrar, analizar y se deben tomar las acciones adecuadas.

11.6.27 Sincronización de relojes

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta (uso del protocolo NTP).

11.7 CONTROL DE ACCESO

11.7.1 Requisitos del negocio para el control de acceso

Definir las directrices para controlar el acceso a la información.

11.7.2 Política de control de acceso

Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio.

11.7.3 Gestión de acceso de los usuarios

11.7.4 Registro de usuarios

Debe existir un procedimiento formal para el registro, modificación y cancelación de las cuentas de usuarios con el fin de conceder, actualizar o revocar el acceso a todos los sistemas y servicios de Información.

11.7.5 Gestión de privilegios

Se debe restringir y controlar la asignación y el uso de privilegios. Se debe aplicar el principio de menor privilegio posible, que consiste en que sólo se otorgan los permisos mínimos necesarios para la ejecución de las funciones. El dueño de la información es el responsable por autorizar los niveles de acceso correspondientes a las cuentas de usuario.

11.7.6 Gestión de contraseñas para usuarios

La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.

11.7.7 Revisión de los derechos de acceso de los usuarios

Se debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios; esta revisión se debe realizar una vez cada 90 días.

11.7.8 Responsabilidades de los usuarios

Esta política define las directrices para evitar el acceso de usuarios no autorizados, robo, puesta en peligro de la información y de los servicios de procesamiento de información.

11.7.9 Uso de contraseñas

Los usuarios deben cumplir con las buenas prácticas en la selección y el uso de las contraseñas:

- Complejidad
- No reutilizar las últimas 5
- Caracteres númericos, alfanuméricos y especiales.
- No incluir nombres o fechas
- Que sea fácil de memorizar para no tener que escribirla

11.7.10 Equipo de usuario desatendido

Los usuarios deben asegurarse que a los equipos desatendidos se les dé la protección apropiada. En las estaciones de trabajo Windows se debe habilitar el control automático de bloqueo con contraseña, para las sesiones que permanecen más de cinco (5) minutos inactivas. Los usuarios deben evitar dejar sus estaciones de trabajo con la sesión abierta.

11.7.11 Política de escritorio despejado y pantalla despejada

Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

- Los empleados deben adoptar la cultura de “escritorio despejado” que consiste en: en los puestos de trabajo sólo deben permanecer los documentos y elementos necesarios para la realización de las labores y en la pantalla solo los iconos propios del sistema.

- Los archivadores y escritorios deben permanecer cerrados con llave.
- No dejar documentos confidenciales a la vista de otras personas.
- No arrojar documentos confidenciales a la basura, estos deben ser destruidos.
- Al finalizar las labores diarias o si el funcionario se va a ausentar de su puesto de trabajo, todos los documentos confidenciales deben ser guardados en sitio seguro.
- No pegue papeles que contengan información confidencial, especialmente contraseñas.
- Mantenga organizado y en orden el puesto de trabajo

11.7.12 Control de acceso a las redes

El objetivo de esta política es evitar el acceso no autorizada a los servicios de red.

11.7.13 Política de uso de los servicios de red

Los usuarios solo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.

- Los usuarios deben tener acceso sólo a los recursos necesarios para la ejecución de sus actividades.
- El servicio de correo electrónico debe ser utilizada exclusivamente para actividades laborales.
- La navegación en Internet debe ser razonable y utilizada con propósitos laborales.
- No se deben utilizar los recursos de la organización para almacenamiento de archivos que contengan música, videos, y cualquier información que no sea de carácter laboral.

11.7.14 Autenticación de usuarios para conexiones externas.

Se deben implementar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.

- Las conexiones de acceso remoto o teletrabajo son exclusivamente para propósitos laborales.
- El acceso a información confidencial debe establecerse bajo los mecanismos apropiados de cifrado.
- No se permite la utilización de cuentas o contraseñas genéricas para las conexiones de acceso remoto.
- Las conexiones de acceso remoto deben ser registradas en los *logs* de auditoría.
- Los acceso remotos a servidores críticos deben contar con múltiples factores de autenticación.

11.7.15 Identificación de los equipos en las redes

Los dispositivos de cómputo y comunicaciones deben tener un nombre lógico que permita al administrador de red identificar la ubicación y responsable del mismo. En caso que por motivos de seguridad así se requiera se debe considerar la validación ya sea por dirección IP o por dirección MAC[6].

11.7.16 Protección de los puertos de configuración y diagnóstico remoto

El acceso lógico y físico a los puertos de configuración y diagnóstico debe estar controlado.

[6] Dirección Física de una estación, (Medium Access Controller)

- El acceso físico a los puertos de configuración y diagnóstico debe estar restringido exclusivamente a los responsables de dichas actividades en los respectivos dispositivos.

- La conexión lógica a los puertos de configuración y diagnostico debe estar controlada con mecanismos de autenticación que únicamente permita su acceso a los responsables de dichas actividades en los respectivos dispositivos.

- En caso de no hacer uso de estos puertos de diagnostico, ellos deben estar deshabilitados.

- Se debe registrar el uso de estos puertos.

11.7.17 Separación en las redes

En las redes se deben separ los grupos de servicios de información, usuarios y sistemas de información. Para lograr esta separación se puede hacer uso de la tecnología VLAN[7] o listas de acceso (ACL) o firewall.

11.7.18 Control de conexión a las redes

Para redes compartidas, en caso de existir, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos del negocio.

Se debe aplicar el principio de menor privilegio posible, que consiste en que sólo se otorgan los permisos necesarios para la ejecución de las funciones, de esta forma la conexión desde y hacia redes compartidas debe ser restringida a quienes requieren el acceso y sólo con privilegios mínimos requeridos.

11.7.19 Control de acceso al sistema operativo

Se debe evitar el acceso no autorizado a los sistemas operativos.

11.7.20 Procedimiento de ingresos seguros

El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.

11.7.21 Identificación y autenticación de usuarios

Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de este usuario. Las cuentas de usuario son de carácter individual e intransferible por lo cual todo funcionario que tenga que utilizar los servicios informáticos debe poseer su propia cuenta de usuario. Todas las cuentas de usuario deben utilizar al menos la validación de la contraseña que también permita autenticarla.

11.7.22 Sistemas de Gestión de contraseñas.

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. En la herramienta o utilidad de administración de usuarios de cada sistema operativo, se debe configurar para que todas las contraseñas de acceso cumplan con las características de complejidad y longitud definidas.

11.7.23 Uso de las utilidades del sistema.

Se debe restringir y controlar estrictamente el uso de programas utilitarios que puedan anular los controles del sistema y de la aplicación. La instalación o utilización de herramientas que eludan los controles definidos dentro del sistema no está permitida.

11.7.24 Tiempo de inactividad de la sesión

Las sesiones inactivas se deben suspender después de un periodo definido de inactividad. En la herramienta o utilidad de administración de usuarios de cada sistema operativo, se debe configurar para que las sesiones con más de diez (10) minutos de inactividad sean suspendidas.

[7] Virtual Local Area Network

11.7.25 Control de acceso a las aplicaciones y a la información.

Esta política tiene como objetivo evitar el acceso no autorizado a la información contenida en los sistemas de información.

11.7.26 Restricción de acceso a la información

Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte de acuerdo con la política definida de control de acceso. Los permisos otorgados dentro de cada sistema deben ser controlados por roles y perfiles de usuario que determinen los niveles de acceso de acuerdo a las funciones desempeñadas por cada usuario. Los formatos de acceso a los sistemas de información deben ser diligenciados y poseer su respectiva aprobación.

11.7.27 Aislamiento de sistemas sensibles

Los sistemas sensibles deben tener un entorno informático dedicado (aislados).

11.7.28 Computación móvil y trabajo remoto

Esta política tiene como objetivo garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

11.7.29 Computación y comunicaciones móviles

Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicación móviles.

11.7.30 Trabajo remoto

Se deben desarrollar e Implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto, en caso de ser necesarias. Estos procedimientos, deben cumplir con los lineamientos de menor privilegio y con los estándares previamente definidos de seguridad. Algunas recomendaciones son:

- Utilizar la tecnología VPN[8]
- Antivirus actualizado
- Manejo adecuado de la información definida como confidencial
- Utilización de la tecnología de cifrado y autenticación
- Personal firewall activado y con su respectivo estándar de configuración

[8] Virtual Private Network

11.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

11.8.1 Requisitos de seguridad de los sistemas de información

Esta política tiene como objetivo garantizar que la seguridad es parte integral de los sistemas de información.

11.8.2 Análisis y especificaciones de los requisitos de seguridad.

Las declaraciones sobre los requisitos de negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben, especificar los requisitos para los controles a nivel de seguridad de la información. Entre ellos se debe exigir que el nuevo sistema de información contemple una estructura efectiva de gestión de contraseñas y sistemas que faciliten el respaldo de la información.

11.8.3 Procesamiento correcto de las aplicaciones

Esta política tiene como objetivo evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

11.8.4 Validación de los datos de entrada

Se deben validar los datos de entrada a las aplicaciones para asegurar que ellos son correctos y apropiados.

11.8.5 Control de procesamiento interno

Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento deliberados.

11.8.6 Integridad del mensaje

Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad de los mensajes en las aplicaciones, así como identificar e implementar los controles adecuados.

11.8.7 Validación de los datos de salida

Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.

11.8.8 Controles criptográficos

Esta política tiene como objetivo proteger la confidencialidad, o integridad de la información. Los protocolos fuertes que se pueden usar son:

- AES 128
- AES 192
- AES 256
- SHA-2

11.8.9 Política sobre el uso de los controles criptográficos

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

11.8.10 Seguridad de los archivos del sistema

Esta política tiene como objetivo proteger la confidencialidad, o integridad de la información.

11.8.11 Control de software operativo

Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. Entre estos controles esta la aprobación por parte del Jefe de Departamento y completar el formato respectivo.

11.8.12 Protección de los datos de pruebas del sistema

Los datos de prueba deben seleccionarse cuidadosamente así como protegerse y controlarse.

11.8.13 Control de acceso al código fuente de los programas

Se deben restringir el acceso al código fuente de los programas.

11.8.14 Seguridad en los procesos de desarrollo y soporte

Esta política tiene como objetivo mantener la seguridad del software y de la información del sistema de aplicaciones

11.8.15 Procedimientos de control de cambios

Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

11.8.16 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Cuando se cambian los sistemas operativos, las aplicaciones críticas para los objetivos de negocio, se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad.

11.8.17 Restricción en los cambios a los paquetes de software

Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.

11.8.18 Fuga de información

Cuando se cambian los sistemas operativos, las aplicaciones críticas para los objetivos del negocio, se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad.

11.8.19 Desarrollo de software contratado externamente

Se debe supervisar y monitorear el desarrollo de software contratado externamente. Esta empresa como proveedor de servicio debe cumplir con requerimientos de seguridad definidos en conjunto.

11.8.20 Gestión de la vulnerabilidad técnica

Esta política tiene como objetivo reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

11.8.21 Control de vulnerabilidades técnicas

Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

11.9 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

11.9.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Esta política tiene como objetivo asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

11.9.2 Reporte sobre los eventos de la seguridad de la información

Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible. Se debe crear y utilizar un procedimiento "**Gestión de Incidentes**".

11.9.3 Reporte sobre las debilidades de la seguridad de la información

Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechosas en los sistemas o servicios.

11.9.4 Gestión de los incidentes y las mejoras en la seguridad de la información

Esta política tiene como objetivo asegurar que se aplica un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información

11.9.5 Responsabilidades y procedimientos.

Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Utilizar y crear un procedimiento "**Gestión de Incidentes**".

11.9.6 Aprendizaje debido a los incidentes de seguridad de la Información

Deben existir mecanismos que permitan cuantificar, analizar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información, con el fin de aprender de estos eventos para prevenirlos a futuro. Ver procedimiento "**Gestión de Incidentes**".

11.9.7 Recolección de evidencia

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas en el cuidado de la evidencia establecidas en la jurisdicción pertinente. Crear y utilizar procedimiento "**Recolección de evidencia**".

11.10 CUMPLIMIENTO

El objetivo de esta política es evitar el incumplimiento por parte de XXX, de las leyes de obligación, reglamentarias o contractuales y de cualquier requisito de seguridad.

11.10.1 Identificación de la legislación aplicable

Todos los requisitos reglamentarios y contractuales pertinentes, así como el enfoque para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información.

11.10.2 Derechos de propiedad intelectual

Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

11.10.3 Protección de los registros

Los registros importantes se deben proteger contra perdida, destrucción y falsificación, de acuerdo con los requisitos reglamentarios, contractuales y del negocio.

11.10.4 Protección de los datos y privacidad de la información personal

Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y si aplica con las cláusulas del contrato.

11.10.5 Prevención del uso inadecuado de los servicios de procesamiento de información

Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para usos no autorizados.

11.10.6 Reglamentación de los controles criptográficos

Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

11.10.7 Cumplimiento con las políticas y normas de seguridad

Los gerentes y directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

11.10.8 Verificación del cumplimiento técnico

Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas y políticas de seguridad.

11.10.9 Controles de auditoria de los sistemas de información

Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos de negocio.

11.10.10 Normatividad

El administrador del sistema o el Oficial de Seguridad no leerá o facilitará a otra persona que lea el contenido de ningún archivo de correo electrónico del personal sin obtener el permiso del usuario, excepto en caso que exista un motivo razonable para hacerlo. Dichos motivos pueden incluir, sin limitarse a ello, mantener la integridad del sistema (tal como la eliminación de virus), cumplir obligaciones legales (tal como citaciones judiciales) y efectuar ciertas funciones de administración del sistema (tal como remitir los mensajes con direcciones erróneas).

12 BIBLIOGRAFÍA

1. ISO/IEC 27001:2013 Sistemas de gestión de la seguridad de la información.
2. ISO/IEC 27001:2005 Sistemas de gestión de la seguridad de la información
3. ISO 27032:2012
4. ISO 27005:2018
5. ISO 31000:2018
6. ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
7. NTC 5254 Gestión del riesgo.