ESTRUCTURA RECOMENDADA PARA EL DOCUMENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013

VERSIÓN 1.0

Tabla de contenido

Info@sisteseg.com

Tabla de ilustraciones

1 Introducción

Se busca 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 Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001 diseñado e implementado para tal fin y, por último, se espera como consecuencia de este proceso que todos los empleados adquieran también un compromiso permanente con la protección y el buen uso de los activos de información de toda la organización, componentes indispensables para lograr la visión y misión organizacional.

El proceso de tomar conciencia de la importancia de proteger y hacer buen uso de los activos de información debe estar dentro de un marco conceptual que permita la mejora gradual en lo relacionado con la seguridad de la información, sin afectar la operación de la compañía y, que por otro lado, no se disminuya la productividad hasta ahora alcanzada por los empleados. También es importante que se consideren los costos, beneficios e implicaciones asociados a cualquier tecnología que se decida implementar de acuerdo al proceso de gestión de riesgos.

Para lograr lo anteriormente expuesto, es decir, el logro de los objetivos de la seguridad de la información según la norma ISO 27001: 2013, este documento establece la estructura que el documento de políticas de seguridad de la información debe poseer para proteger adecuadamente los activos de información de acuerdo a estándares internacionales (ISO 27005, ISO 27031, ISO 27032, PCI DSS V 3.2) que han sido probados en grandes e importantes empresas a nivel mundial. Es así que, este documento se apoya en las mejores prácticas en seguridad de la información orientadas a que se pueda operar de una forma continua y segura todos los activos de información críticos, garantizando así el cumplimiento de su misión organizacional.

2 Alcance de las políticas de seguridad de la información

Las políticas de seguridad de la información según la norma ISO 27001:2013, deben aplicar a todos los activos de información. Estas políticas también aplicarán también a todos los empleados, consultores, contratistas, temporales o terceras partes que accedan a los activos de la información. Los consultores, contratistas, o terceras partes estarán sujetos a similares requerimientos de seguridad que los empleados.

Los empleados, contratistas, temporales o terceras partes estarán obligadas a continuar protegiendo la información, cumpliendo las políticas de seguridad inclusive después de terminar su relación con la organización.

3 Propósitos de las políticas ISO 27001:2013

El propósito de las Políticas de Seguridad de la Información ISO 27001 debe ser proteger los activos de información de las amenazas internas o externas, bien sean intencionales, naturales o accidentales.

Será política de la organización garantizar, entre otros:

1. **Confidencialidad** de la información, de manera que únicamente usuarios autorizados tengan acceso.
2. **Integridad** de la información, evitando su alteración no autorizada.
3. **Disponibilidad** de la información, asegurando su presencia cuando sea requerida por usuarios debidamente autorizados y en un tiempo razonable de respuesta.
4. **Cumplimiento** de las leyes y regulaciones.
5. **Entrenamiento** a todos los empleados en el tema de seguridad de la información.
6. **Cumplimiento** de las obligaciones contractuales con nuestros clientes y proveedores.

4 Alcance del documento

Este documento comprende los siguientes aspectos:

1. Política general de la seguridad ISO 27001:2013
2. Políticas por dominios
3. Violaciones a la política
4. Revisiones de la política
5. Roles y responsabilidades
6. Normas
7. Procedimientos asociados
8. Estándares de configuración
9. Guías y recomendaciones
10. Formatos
11. Manual de usuarios

5 Estructura proyectada del documento de políticas ISO 27001

A continuación se presenta una figura con la estructura proyectada del documento de políticas de seguridad de la información:

Ilustración 1. Estructura del documento de políticas ISO 27001.

6 Política general ISO 27001:2013

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

La política general de la seguridad de la información refleja el compromiso de la organización con la protección de los activos de información considerando los siguientes aspectos:

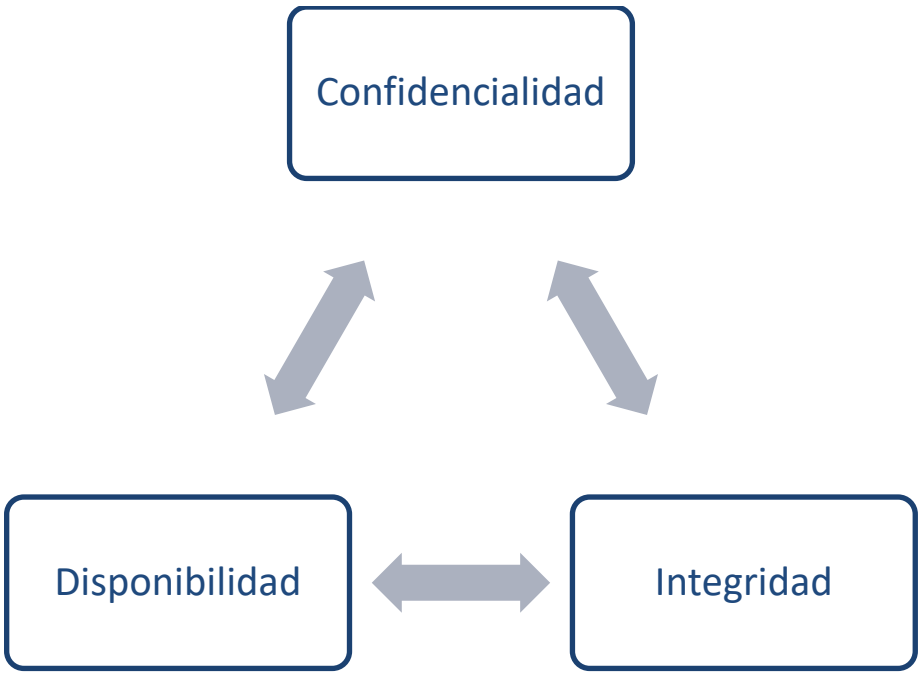

Ilustración 2. Objetivos de la seguridad de la información.

7 Políticas por dominios de ISO 27001:2013

Los dominios considerados, teniendo en cuenta el estándar ISO 27001:2013 son:

Política de seguridad: Constituye el lineamiento de alto nivel con relación a la protección de activos de información siguiendo los lineamientos dados por ISO 27001:2013.

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

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

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.

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

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

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.

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.

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.

8 Violaciones a la política ISO 27001

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.

9 Revisiones de la política ISO 27001

Cuando las políticas estén disponibles deben ser modificadas si existieran cambios importantes en los procesos de negocio o en su infraestructura tecnológica, de no haber cambios, se debe realizar su revisión anualmente.

10 Roles y responsabilidades

Dentro del marco de SGSI según la norma ISO 27001 se debe contar con la asignación de un grupo de personas con diferentes roles y responsabilidades para realizar las actividades asociadas con el diseño, actualización, documentación, divulgación y futura aprobación de las políticas y normas de seguridad de la información.

11 Normas

Las normas corresponden a los aspectos específicos que se desprenden de las políticas de seguridad de la información. Estas normas serán de cumplimiento obligatorio por parte de los funcionarios de la organización.

12 Procedimientos asociados

Los procedimientos son las actividades detalladas (paso a paso), documentadas y específicas relacionados con las políticas de seguridad de la información.

13 Estándares de configuración

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.

Los estándares de configuración corresponden a los parámetros específicos por plataforma con el fin de garantizar el cumplimiento de los objetivos de la seguridad de la información.

14 Guías y recomendaciones

Cuando alguna actividad sea conveniente realizarla, sin ser necesariamente de cumplimiento obligatorio, se puede generar un documento de mejores prácticas, guías o recomendaciones con el fin de mejorar en nivel de seguridad asociado con esta actividad.

15 Formatos

Para poder realizar de manera precisa y formal algunas de las actividades relacionadas con la seguridad de la información, será conveniente apoyarse en una serie de formatos tanto electrónicos como físicos los cuales deberán ser completados para cumplir con la política de seguridad.

16 Manual de usuarios

Los usuarios conforman una parte importante dentro de la implementación de un sistema de gestión de la seguridad de la información. Por tal motivo, se debe contar con un documento de fácil lectura y comprensión, para que los funcionarios de la organización y los usuarios de los sistemas, cumplan con la preservación de la confidencialidad, integridad y disponibilidad de la información.

17 Bibliografía

1. ISO/IEC 27001: 2013 Sistemas de gestión de la seguridad de la información.
2. ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
3. ISO/IEC 17799 Código de práctica para la gestión de la seguridad de la información.
4. NTC 5254 Gestión del riesgo.
5. ISO 27031
6. ISO 27032

Anexos

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 ISO 27001: Sistema de Gestión de la Seguridad de la Información.

Política de Seguridad ISO 27001: 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 propiedad de la organización.

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

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

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:

1. Una noticia que escuchamos por la radio.

2. Una señal de tráfico que advierte un peligro.
3. 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 IT.

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 pública 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.