Unidad 3 / Escenario 5

Lectura fundamental

Políticas de seguridad de la información: primer paso para la gestión de seguridad

Contenido

1 Introducción
2 Modelos de gestión con enfoque en procesos
3 Requerimiento de políticas de seguridad de la información
4 Diseño y estructura de las políticas de seguridad de la información
5 Ejemplo diseño y estructuración de una política

Palabras clave: modelo ISO 27001, modelo O-ISM3, políticas de seguridad.

Introducción

Cuando hablamos de una política hacemos referencia a todo aquello que es de obligatorio cumplimiento por encontrarse aprobado por un ente de nivel superior. Las políticas permiten que los miembros de una organización orienten sus esfuerzos en un mismo sentido y regulen el comportamiento de los diferentes actores de un sistema.

Para los sistemas de gestión que operan bajo normas ISO, la política define el papel del tópico del sistema; por ejemplo, el papel de la seguridad de la información en el sistema de gestión de seguridad de la información dentro de la organización. En otras palabras, la política es el corazón del sistema y, por tanto, su diseño, estructuración, socialización, cumplimiento y permanente revisión son actividades que se realizan de manera independiente y con un objetivo específico.

Así pues, este Escenario amplía el concepto de política de seguridad de la información, su diseño y estructura orientada a un sistema de gestión basado en procesos, analizando los modelos propuestos por la Norma ISO 27001 y el modelo de madurez de seguridad de la información O-ISM3.

1. Modelos de gestión con enfoque en procesos

1.1. Norma ISO 27001

La norma ISO 27001 hace parte del grupo de normas ISO que se caracteriza por brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema basado en procesos. Es importante aclarar que para las normas ISO un proceso es cualquier actividad que use recursos cuya gestión permita la transformación de entradas en salidas y la aplicación de un sistema de proceso dentro de una organización, junto con la identificación de interacciones entre estos procesos; su gestión se denomina enfoque basado en procesos (Instituto Colombiana de Normas Técnicas y certificaciones, 2013).

El enfoque basado en procesos de la norma ISO 27001 indica a las empresas, que esperan adoptar esta norma para gestionar seguridad, la importancia, en primera instancia, de comprender las necesidades y requerimientos de seguridad de la información de la empresa y, a partir de allí, establecer la política y los objetivos de seguridad del sistema.

Para estructurar todos los procesos del sistema de gestión de seguridad de la información propuestos por la norma ISO 27001, esta ha adoptado el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA).

En la Figura 1 se puede observar el resumen del modelo con enfoque por procesos. Cabe resaltar que los requisitos y expectativas de seguridad son conceptos diferentes: el requisito está orientado al mínimo que debe tener el sistema (por ejemplo, que un incidente de seguridad de la información no cause un daño mayor a nivel financiero), mientras que una expectativa es lo que se espera del sistema (por ejemplo, para el mismo incidente se espera que exista personal capacitado para minimizar el impacto). En otras palabras, si se materializa el riesgo, no debe causar daño financiero y se espera contar con personal capacitado para atender el impacto del riesgo que no debe ser, por ningún motivo, financiero.

Adicionalmente, las partes interesadas son transversales al sistema, aunque sean diferentes para establecer requisitos o expectativas y gestionar la seguridad. Por tal motivo, se deben identificar claramente a los interesados del SGSI e informar sobre el funcionamiento del sistema en cualquiera de los ciclos que se encuentre.

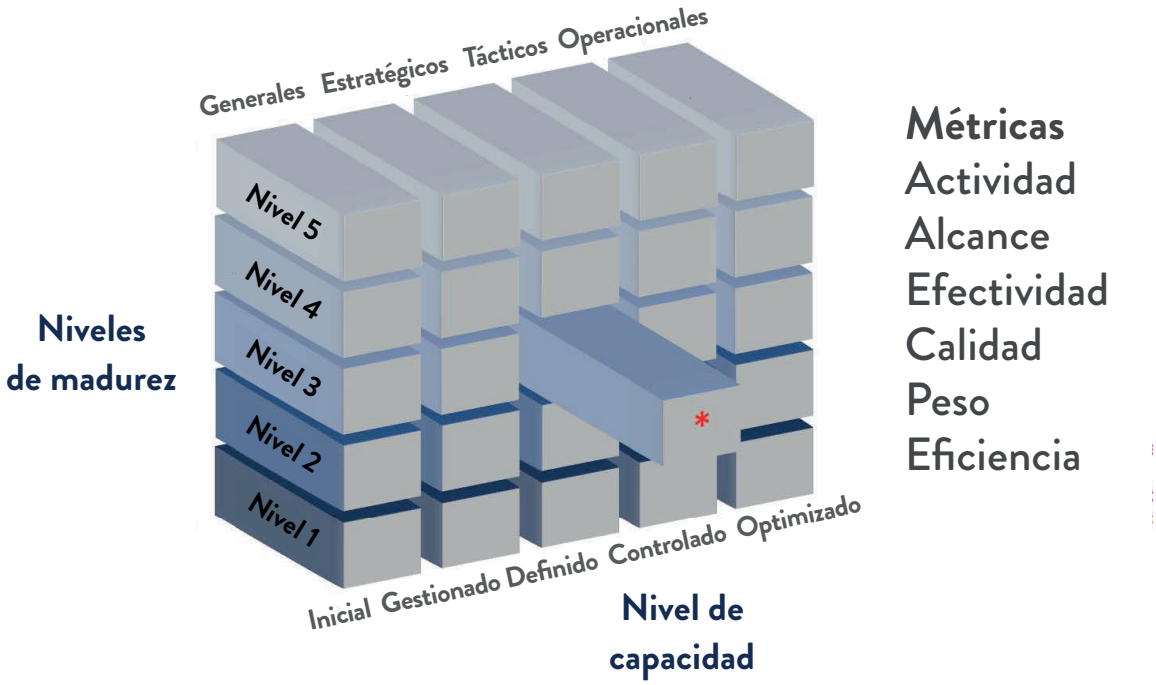
Figura 1. Modelo PHVA aplicado a los procesos de SGSI

Fuente: elaboración propia

1.2. Modelo O-ISM3

Como vimos en la unidad anterior, el modelo O-ISM3 tiene un enfoque en procesos, utilizando otros conceptos como las capacidades y la madurez. Estos conceptos son la base del modelo, puesto que indican qué tan preparada se encuentra una organización para implementar un sistema de gestión de seguridad de la información (capacidades) e identifica el nivel en el que se encuentra para avanzar hacia el estado que quiere lograr (madurez).

En la Figura 2 podemos observar el resumen del modelo en cuanto a las variables que utiliza para evaluar una empresa que lo adopta y que aplica a la certificación Nivel 3 de madurez, con un nivel de capacidad definido. Esto quiere decir que la empresa ha logrado planear y monitorear los procesos generales en su totalidad exigidos por el modelo, los procesos estratégicos, tácticos y operacionales correspondientes a un nivel 3 y que cumple como mínimo las métricas actividad, alcance y efectividad, que son exigidas para el nivel de capacidad llamado "definido", como se muestra en la Tabla 1.



* Alta inversión en el modelo. Procesos generales, tácticos, operacionales y estratégicos implementados según la exigencia del modelo para nivel de madurez 3 y según las métricas actividad, alcance y efectividad.

Figura 2. Estructura general modelo O-ISM3. Ejemplo nivel 3 de madurez alcanzado

Fuente: elaboración propia

Tabla 1. Estructura del Modelo O-ISM3

Nivel de capacidad		Inicial	Gestionado	Definido		Controlado		Optimizado
Actividades de gestión		Auditar, certificar	Probar (evaluar)	Planear	Monitorear	Analizar beneficios	Mejorar la calidad	Mejorar el desempeño
Documentación		*	*	*	*	*	*	*
Tipo de Métrica	Actividad			*	*	*	*	*
	Alcance			*	*	*	*	*
	Efectividad			*	*	*	*	*
	Calidad					*	*	*
	Carga (peso)							*
	Eficiencia							*

Fuente: elaboración propia

2. Requerimiento de políticas de seguridad de la información

El apartado anterior expuso dos modelos para la gestión de seguridad de la información. Estos modelos tienen características comunes, como el enfoque en procesos para la gestión, aunque proponen mecanismos diferentes para ello. El modelo PHVA es comúnmente aceptado como referente para la gestión de seguridad de la información, puesto que la norma ISO 27001 lo declara referente de manera explícita, mientras que el modelo O-ISM3 lo define implícitamente al indicar como parte de las actividades de gestión aspectos como planear, monitorear, mejorar etc., que se desarrollan en las capacidades alcanzadas por la empresa.

En otras palabras, podemos indicar que el modelo O-ISM3 es compatible con el estándar ISO 27001:2013, pero utiliza un enfoque diferente. La familia de normas ISO 2700 presenta la gestión de seguridad de la información como un proceso único que se apoya en otros subprocesos para la implementación de controles que permiten lograr los objetivos definidos para el sistema. Por el contrario, el enfoque de O-ISM3 es definir y medir lo que las personas hacen en las actividades que respaldan la seguridad; a este respecto, podemos considerar que ISO / IEC 27001 cumple con los requisitos de un auditor, mientras que O-ISM3 cumple con las necesidades de un gerente.

Los dos modelos utilizan en común el término de política de seguridad de la información como elemento de entrada para la gestión de seguridad. En este sentido, podemos considerar que la definición de la política, su implementación, revisión y mejora es parte fundamental para la gestión de seguridad de la información y aquí radica la importancia de diseñarla, estructurarla, socializarla, cumplirla y revisarla.

2.1. Requerimientos de una política de seguridad de la información norma ISO 27001

Como se ha explicado, la norma ISO 27001:2013 tiene un enfoque basado en procesos utilizando el ciclo PHVA. La norma presenta cómo el ciclo PHVA es utilizado para definir, estructurar, cumplir y revisar la política de seguridad de la información, eje fundamental del sistema de gestión de seguridad de la información SGSI.

En la Tabla 2 se presenta el resumen de lo propuesto por la norma.

Tabla 2. Política de seguridad de la información según el ciclo PHVA

Fase del CICLO PHVA	Requerimiento para cumplir con la fase
Planificar (establecer el SGSI)	Se debe establecer una política de seguridad de la información que incluya objetivos, procesos y procedimiento, para el tratamiento de los riesgos que se encuentren alineados con el negocio.
Hacer (implementar y operar el SGSI)	Implementar y operar la política de acuerdo con la planeación realizada en el punto anterior.
Verificar (hacer seguimiento y revisar el SGSI)	Medir y evaluar dónde aplica el desempeño del proceso contra la política para informar a las áreas interesadas.
Actuar (mantener y mejorar el SGSI)	Con los resultados anteriores, ejecutar las acciones preventivas y correctivas necesarias.

Fuente: elaboración propia

En términos generales y referentes a políticas, la norma ISO 27001 propone lo indicado en la Tabla 3.

Tabla 3. Actividades a realizar para implementar políticas de seguridad según la norma ISO 27001

Fase de implementación NTC-ISO/IEC 27003	
5. Obtener la aprobación de la dirección	
Actividad, referencia NTC-ISO/IEC 27003	**Salida documentada**
Reunir los objetivos de negocio	Lista de objetivos corporativos del negocio.
Definir el SGSI preliminar	Descripción del alcance preliminar del SGSI. Definición de los roles y responsabilidades del SGSI.
Crear el caso de negocio	El caso junto con el plan de proyecto.
Aprobación de la dirección	Documento firmado con autorización.

Fase de implementación NTC-ISO/IEC 27003	
6. Definir el alcance y política del SGSI.	
Desarrollar la política del SGSI.	Política del SGSI.
7. Realizar el análisis de la organización	
Definir los requisitos de seguridad de l a información.	Lista de los recursos necesario por parte de la organización que contengan información como requisito.
8. Realizar la valoración de riesgos y seleccionar las opciones para su tratamiento	
Obtener la aprobación de la dirección para la implementación.	Riesgos y sus opciones de tratamiento identificadas.
Aprobación de los riesgos residuales por parte de la dirección.	Documento firmado con la aprobación documentada de los riesgos residuales propuestos por parte de la dirección.
Autorización de la dirección para la implementación del sistema.	Documento firmado con la autorización para implementar y operar el sistema.
Preparar una declaración de aplicabilidad.	Declaración de aplicabilidad.
9. Diseñar el SGSI	
Diseñar organigrama de seguridad.	Descripción de roles, responsabilidades y cargos.
	Enumerar documentos relacionados con el sistema.
	Indicación de plantillas y su archivo para el sistema.
	Documento de la política de seguridad de la información.
	La línea de base de las políticas y procedimientos de la seguridad de la información.
	Un programa de formación y toma de conciencia.
Producir el plan del proyecto final.	Plan del proyecto de implementación aprobado por la dirección para los procesos de implementación.
El plan del proyecto final del SGSI.	Un plan específico para el proyecto de implementación del SGSI de la organización.

Fuente: elaboración propia

2.2. Requerimientos de una política de seguridad de la información modelo O-ISM3

El contexto del modelo se basa en la visión global que se ha definido para los sistemas de información, la cual indica que la necesidad principal es proteger los sistemas de las amenazas que regularmente les causan daños. En el contexto empresarial, los profesionales de la seguridad de la información generalmente abordan esta necesidad dividiéndola en las áreas definidas, como lo muestra la siguiente tabla.

Tabla 4. Áreas para la formulación, implementación y mantenimiento de política de seguridad de la información

Área	Requerimiento
Gestión de riesgos	Identificar y estimar los niveles de riesgo (probabilidad de ocurrencia e impacto) para que los gerentes tomen decisiones con respecto al tratamiento que se realizará sobre estos (aceptar, mitigar, transferir), mediante los controles necesarios de acuerdo con los resultados del análisis costo beneficio. Estas decisiones son consideradas insumos para el diseño y formulación de las políticas de seguridad de la información, pues describen cómo se gestionará la seguridad de la información.
Controles de seguridad	A partir de su política empresarial y con base al resultado de gestión de riesgos, se estructura e implementa la política de seguridad de la información, que va alineada a la política corporativa y define los controles que deben utilizarse para garantizar el cumplimiento de esta.
Gestión de seguridad	Una vez implementada la política se debe garantizar su cumplimiento, soporte y mantenimiento a través de los mecanismos definidos para la gestión de seguridad de la información. En otro sentido, la gestión de la seguridad de la información implica el apoyo y el mantenimiento de la política de seguridad definida.

Fuente: elaboración propia

Adicionalmente, el modelo indica que la selección de procesos sugeridos por él, al igual que las métricas a implementar, dependerá de la definición, implementación y mantenimiento de la política definida. A diferencia de la norma ISO 27001, en la cual todos los controles son de obligatorio cumplimiento para la certificación, el modelo O-ISM3 permite escoger los que se consideren necesarios de acuerdo con las necesidades de seguridad de la información de la empresa, definidas en la política, teniendo como referente el nivel de madurez que se quiere certificar.

Al igual que la norma ISO 27001, el modelo muestra que la política de seguridad de la información depende del contexto de la empresa, desde el cual se pueden generar otras políticas que, de acuerdo con el nivel de madurez, deben ser documentadas. En la siguiente tabla se presentan las políticas con sus respectivos documentos y procesos.

Tabla 5. Resumen de políticas para el modelo O-ISM3

Grupo de Procesos	Proceso	Documento
Procesos genéricos	Gestión del conocimiento (GP-1)	Revisar y aprobar la política de seguridad de la información (GP-011).
Procesos genéricos	Gestión del conocimiento (GP-1)	Distribución de la política (GP-013).
Procesos genéricos	Gestión del conocimiento (GP-1)	Política de control del ciclo de vida (GP-017).
Procesos genéricos	Gestión del conocimiento (GP-1)	Política de control de acceso ambiental (GP-018).
Procesos genéricos	Gestión del conocimiento (GP-1)	Política de gestión de disponibilidad (GP-019).
Procesos genéricos	ISMS y auditoría del negocio (GP-2)	Auditoría de la política (criterio, alcance, reglas) (GP-021).
Procesos genéricos	ISMS y auditoría del negocio (GP-2)	Política de prueba y auditoría (GP-022).
Procesos genéricos	ISMS y auditoría del negocio (GP-2)	Política de seguridad de la información (GP2-024).
Procesos genéricos	Implementando O-ISM3 (GP-3)	Plantilla de política de seguridad de la información (GP-033).
Procesos genéricos	Complementarios	Política de supervisión (GP-01B), política de manejo de incidentes (GP-01A), política de manejo de personal (GP-01C), política de manejo de uso aceptable (GP-01D), política de gestión de riesgos (GP-01G).
Procesos estratégicos	Establecer las reglas para definición de las obligaciones (SSP-4)	Plantilla de política TPSRSR (GSSP-041).
Procesos tácticos	Definir metas y objetivos de seguridad (TSP-3)	Plantilla de política de acuerdo con el código de relación de terceros (TSP-034).
Procesos operativos	Gestión de inventario (OSP-3)	Política de nombres de activos OSP-032.

Fuente: elaboración propia

3. Diseño y estructura de las políticas de seguridad de la información

Como se señaló, el diseño y la estructura de la política depende del modelo que se espere implementar y, en términos generales, corresponden a las fases o niveles que este defina.

Por ejemplo, para el modelo ISO 27001, el diseño y estructura corresponden a las fases P y H del ciclo PHVA, es decir planificar y hacer. De aquí en adelante, el enfoque va a ser en este modelo para lo referente a la política de seguridad de la información, puesto que es fácil de entender para el desarrollo de una política. Se puede replicar al modelo O-ISM3, en el cual se establecen muchas políticas en los procesos genéricos y referentes a varios puntos en seguridad.

3.1. Diseño de una política

Casi siempre, una política es la declaración de la intención y objetivo general expresados formalmente por la dirección (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

El contenido de una política orienta las acciones y decisiones concernientes al tema que trata la política, por ejemplo, seguridad, calidad, etc. Una organización puede tener varias políticas, una para cada una de sus áreas importantes de actividad. Algunas políticas son independientes entre sí, mientras que otras tienen una relación jerárquica, como comúnmente sucede en el área de seguridad; de manera habitual, la política de seguridad de la información es la política de mayor nivel (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

Las políticas pueden sustentarse unas con otras dependiendo de la organización y de lo que se quiera lograr con la implementación de un sistema de gestión; en este caso, el sistema de gestión de seguridad de la información SGSI.

En lo referente a la seguridad de la información, la política de seguridad puede estar sustentada en otras políticas detalladas sobre temas específicos, como el control de acceso, las relaciones con terceros, etc., tal como se expuso en una sección anterior (Modelo O-ISM3). La norma ISO 27002:2013 define este tipo de políticas. Recordemos que la norma ISO 27001 indica qué se debe hacer, la norma ISO 27002 indica cómo hacerlo y la norma ISO 27003 es una guía para la implementación del modelo. Por esto se mencionan las tres normas en lo referente a la política de seguridad.

3.1.1. Jerarquía de políticas

Para el caso concreto de la Norma ISO27001, esta exige que la empresa cuente con una política de seguridad de la información y una política para el sistema de gestión de seguridad de la información.

En este sentido, puede llegar a ser confusa la cantidad de políticas que se requieren para temas referentes a seguridad de la información con respecto a la norma ISO.

En términos prácticos, la jerarquía de las políticas de seguridad de la información se puede definir como se aprecia en la Figura 3. En esta se observa que las políticas detalladas sustentan las políticas del nivel superior y esta es la manera propuesta para el diseño de políticas de seguridad de la información: identificar el nivel de jerarquía de acuerdo con la empresa.

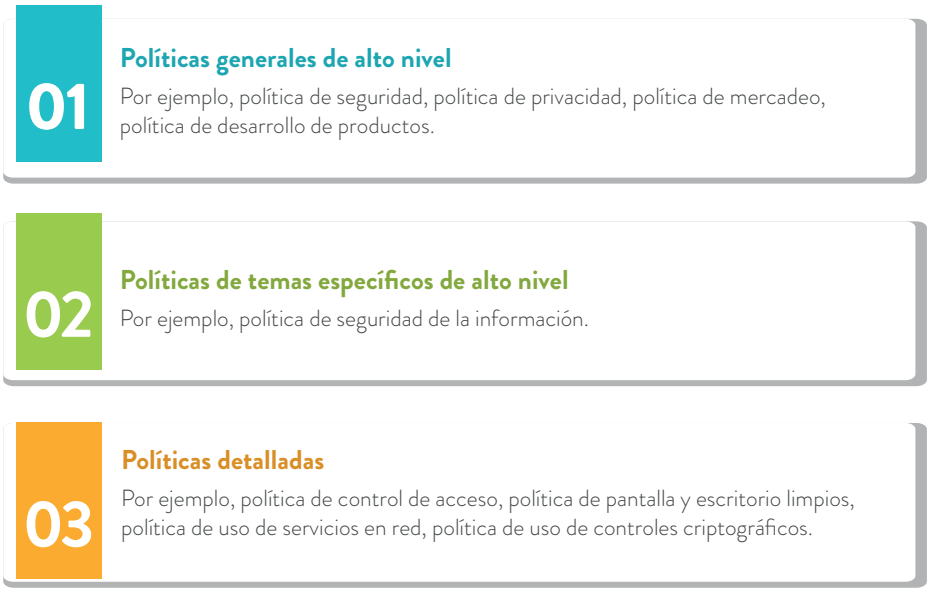


Figura 3. Jerarquía de las políticas

Fuente: elaboración propia

El contenido de las políticas se basa en el contexto en el que opera una organización. Por tal motivo, cuando se genera cualquier política, su diseño debe contener los aspectos indicados en la Figura 4. Este diseño permite que la política sea clara, precisa y específica para el tema abordado.

Figura 4. Contenido de una política

Fuente: elaboración propia

3.2. Estructura de una política

En la tabla 6 se puede identificar la estructura que debe tener una política de seguridad de la información.

Tabla 6. Estructura de una política de seguridad de la información

Resumen de la política	Visión general.	**Principios**	Describe las reglas acerca de las acciones y las decisiones para lograr los objetivos
Introducción	Breve explicación del tema de la política.	**Responsabilidades**	Describe quién es el responsable de las acciones para cumplir los requisitos de la política
Alcance	Describe las partes o actividades de una organización que se ven afectadas por la política.	**Resultado clave**	Describe los resultados del negocio si los objetivos se cumplen.
Objetivos	Describe la intención de la política.	**Políticas relacionadas**	Describe otras políticas pertinentes para el logro de los objetivos.

Fuente: elaboración propia

4. Ejemplo de diseño y estructuración de una política

El siguiente es un ejemplo de una política de seguridad de la información, que ilustra su estructura y contenido.

» **Resumen de la política**

La información siempre debe estar protegida, cualquiera que sea su forma, ya sea que se haya compartido, esté almacenada o que se haya comunicado (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

» **Introducción**

La información puede existir de diferentes formas: escrita o impresa en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, presentada en películas o informada personalmente (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

La seguridad de la información es la protección de esta contra una amplia variedad de amenazas, para asegurar la continuidad del negocio, minimizar su riesgo y maximizar el retorno sobre la inversión y oportunidades de negocio (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

» Alcance

Esta política sustenta la política de seguridad general de la organización y comprende a toda la organización (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

» Objetivos de seguridad de la información

1. Los riesgos de seguridad de la información estratégicos y operativos se entienden y se tratan de manera que sean aceptables para la organización.
2. La confidencialidad de la información del cliente, los planes para desarrollo del producto y mercadeo están protegidos.
3. La integridad de los registros contables está reservada.
4. Los servicios de red públicos y las redes internas cumplen las normas de disponibilidad (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

» Principios de seguridad de la información

1. Los detalles del enfoque asumido para la evaluación del riesgo se encuentran en la política del SGSI.
2. Todo el personal debe conocer y rendir cuentas sobre la seguridad de la información en cuanto sea pertinente para su rol de trabajo.
3. Se deben tomar medidas para consolidar controles de seguridad de la información en procesos de gestión de proyectos y operativos.
4. En toda la gestión de sistemas de información se tendrán en cuenta las posibilidades de fraude asociado a abuso en los sistemas de información.
5. Están disponibles los reportes del estado de seguridad de la información.
6. Se hace seguimiento de los riesgos de seguridad de la información y se toman acciones cuando los cambios den como resultado riesgos que no sean aceptables.
7. Los criterios para la clasificación y la aceptabilidad de riesgos se encuentran en la política de SGSI.
8. No se toleran situaciones que puedan poner a la organización en situación de violación de leyes y reglamentos (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

» Responsabilidades

1. El equipo de la alta dirección es responsable de garantizar que la seguridad de la información tenga el enfoque definido por la empresa.
2. Cada director es responsable de garantizar que la seguridad de la información tenga el enfoque definido por el sistema.
3. El jefe de seguridad asesora al equipo de alta dirección, brinda el apoyo respectivo a la organización y asegura que los informes con respecto al sistema de seguridad de la información se encuentren disponibles.
4. Todos los miembros del personal tienen responsabilidades de seguridad de la información como parte de su trabajo (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

» Resultados clave

1. Los incidentes de seguridad de la información no dan como resultado costos considerables e inesperados por una interrupción grave en los servicios y en las actividades del negocio.
2. Se conocen las pérdidas por fraude, que están dentro de los límites aceptables.
3. La aceptación de productos o servicios por parte de los clientes no se ve afectada por problemas acerca de la seguridad de la información (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

» Políticas relacionadas

Las siguientes políticas detalladas brindan principios y orientación sobre aspectos de seguridad de la información:

1. La política del sistema de gestión de seguridad de la información (SGSI).
2. La política de control de acceso.
3. La política de *software* no autorizado.
4. La política concerniente a la obtención de archivos de software de redes externas o a través de ellas.
5. La política concerniente al código móvil.
6. La política de respaldo.
7. La política concerniente al intercambio de información entre organizaciones.

8. La política concerniente al uso aceptable de instalaciones de comunicaciones electrónicas.
9. La política de retención de registros.
10. La política sobre el uso de servicios en red.
11. La política concerniente a informática y comunicaciones móviles.
12. La política sobre teletrabajo.
13. La política sobre el uso de controles criptográficos.
14. La política de conformidad.
15. La política sobre licencias de *software*.
16. La política sobre disposición de *software*.
17. La política sobre la privacidad y protección de datos.

Todas estas políticas apoyan:

- La identificación de riesgos mediante el suministro de una línea de base de controles, que se pueden usar para identificar brechas en los diseños e implementación de los sistemas.
- El tratamiento de riesgos mediante el apoyo para la identificación de tratamiento para las vulnerabilidades y amenazas identificadas.

Tanto la identificación como el tratamiento de riesgos son procesos definidos en la selección de la política denominada *Principios* (Instituto Colombiano de Normas y Técnicas y Certificación, 2013).

Referencias

Instituto Colombiano de Normas y Técnicas y Certificación. (2013). *Guía Técnica Colombiana GTCISO/IEC 27003*. Bogotá, Colombia: ICONTEC.

Instituto Colombiana de Normas Técnicas y certificaciones. (2013). *Norma Técnica Colombiana NTCISO/IEC 27001- 0.2*. Bogotá, Colombia: ICONTEC.

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Teoría de la Seguridad

Unidad 3: Políticas de seguridad de la información

Escenario 5: Diseño y estructuración de una política deseguridad

Autor: Alexandra Peña Daza

Asesor Pedagógico: Angie Viviana Laitón Fandiño

Diseñador Gráfico: Henderson Jhoan Colmenares

Asistente: Alejandra Morales