Unidad 3 / Escenario 6

Lectura fundamental

Política de seguridad de la información eficaz: es clara, todos la entienden y la aplican

Contenido

Palabras clave: sensibilización, indicadores, medición, política de seguridad, mejora continua.

Introducción

Como ya se expuso, las políticas de seguridad de la información se caracterizan por contar con una estructura clara y abarcan lo referente al negocio y al enfoque de seguridad que se quiera brindar la organización.

Así, la política no es un elemento estático y único, sino que, por el contrario, es un ejercicio continuo que debe ser implementado, revisado y mejorado de manera paulatina y útil para la empresa.

En consecuencia, es de vital importancia definir claramente la manera como se implementa, revisa y modifica la política dentro del sistema de gestión definido, puesto que es la ruta de navegación de este y, por tanto, su cumplimiento es un indicador de su eficacia.

Por tanto, este Escenario expone los elementos que suelen utilizarse para la implementación, revisión y mejora de la política de seguridad de la información dentro del marco de la Norma ISO 27001 y su ciclo PHVA.

1. Implementación de una política de seguridad de la información

A nivel de normas de la familia ISO 27000, la implementación de una política parte de su diseño y definición, que están enmarcados en el contexto que se describe a continuación:

Anexo a objetivos de control y controles 27001:2013 y Norma ISO 27002:2013

Este anexo indica los controles que se deben evidenciar para el cumplimiento de la norma. En la Tabla 1 se presentan los controles específicos para cumplir con la política de seguridad.

Tabla 1. Anexo dominio 5, Norma ISO 27001:2013

A5	Políticas de la seguridad de la información	
A5.1	{Nombre "Enfoque de la política"}	
Objetivo: Aquí se describe el objetivo de la política. Para revisarlo se sugiere al estudiante consultar la Norma ISO 27001:2013		
A5.1.1	Políticas para la seguridad de la información	Control: la norma define cuál es el control que se debe aplicar para cumplir con el requerimiento. Para consultarlo, revisar la Norma ISO 27001:2013.
A5.1.2	Revisión de las políticas para la seguridad de la información	Control: la norma define cuál es el control que se debe aplicar para cumplir con el requerimiento. Para consultarlo, revisar la Norma ISO 27001:2013.

Fuente: elaboración propia

Este anexo está alineado con lo establecido en la Norma ISO 27001:2013, Numeral 4, el cual indica, en términos generales, que la organización debe definir, implementar, ejecutar, realizar seguimiento, revisar y mantener un sistema de gestión de seguridad de la información que se encuentre documentado de acuerdo con las actividades que realice la empresa y la definición de los riesgos de esta. Para los propósitos de esta norma, el proceso usado se basa en el modelo PHVA (ICONTEC, 2013).

En la Tabla 2 se indican los numerales específicos de las normas ISO 27001:2013 e ISO 27003:2013, en los cuales se señala lo que debe cumplir la empresa para la implementación de una política de seguridad de la información.

Tabla 2. Resumen de la implementación de políticas

Numeral general	Numeral específico	Consideraciones
4.2 Establecimiento y gestión del SGSI ISO 27001:2013	4.2.1 Establecimiento del SGSSI	En este numeral se indican los aspectos que la organización debe cumplir en lo referente al establecimiento del SGSI, como el alcance del sistema, la política que incluya un marco de referencia y los requisitos de la empresa, entre otros. Para ampliar la información se debe revisar la norma ISO 27001: 2013 Numeral 4.2.1.
4.3 Requsitos de documentación ISO 27001:2013	4.3.1 Generalidades	La documentación del SGSI debe incluir: Requisitos de negocio, política del sistema, objetivos, alcances, procedimiento y controles que apoyan el sistema, informe de valoración de riesgos, plan de tratamiento de riesgos, procedimiento para garantizar la eficiencia del plan, operación y control del sistema. Para ampliar la información se debe revisar la norma ISO 27001: 2013, Numeral 4.3.1.
6. Definir el alcance, los límites y la políticas del SGSI ISO 27003:2013	6.1 Panorama general de la definición del alcance, los límites y la política del SGSI	Para lograr la aprobación de la dirección para la implementación, se debe definir el alcance que va asociado al caso de negocio y el plan del proyecto. Para definir el alcance se requiere documentar los numerales 4.2.1, indicar los alces a nivel de tecnología, los recursos físicos, entre otros. Para ampliar la información se debe revisar la Norma ISO 27001: 2013 Numeral 6.1.

Fuente: elaboración propia. Adaptado de Icontec (2013)

2. Desarrollar la política del SGSI y obtener la aprobación de la dirección

Para una efectiva implementación de la política es recomendable la planeación de su diseño, junto con la aprobación de la dirección. Para ello se sugiere seguir la guía presentada en la Norma ISO 27003:2013, apartado 6.6, que define el proceso de la siguiente manera:

» **Entrada**

a. Integrar cada uno de los alcances y límites para obtener el alcance y los límites del SGSI.

b. Aclarar las prioridades de la organización para desarrollar un SGSI y establecer los objetivos para implementarlo.

c. Crear el caso de negocio y el plan de proyecto para su aprobación por la dirección. Los siguientes elementos deben estar documentados:

- Los requisitos y las prioridades de seguridad de la información de la organización.
- El plan del proyecto inicial para la implementación del SGSI con sus hitos como, por ejemplo, la evaluación del riesgo, la implementación, las auditorías internas y la revisión por la dirección (ICONTEC, 2013).

Como se puede apreciar, como entrada se sugiere la definición de un proyecto para la implementación no solo de la política, sino también para la definición el Sistema de Gestión de Seguridad de la información.

» **Guía**

Se recomienda considerar los siguientes aspectos al definir la política del SGSI:

a. Establecer los objetivos del SGSI con base en los requisitos y en las prioridades de seguridad de la información de la organización.

b. Definir el enfoque general y una guía para lograr los objetivos del SGSI.

c. Considerar los requisitos legales a nivel de legislación del sector de la empresa y contratos que haya adquirido o esté próxima a conseguir.

d. Precisar la gestión de riesgo en el contexto de la organización.

e. Determinar cómo se realizará la gestión y la valoración de riesgo. Para realizarlo, se debe revisar la norma.

f. Indicar el rol de la alta dirección con respecto al sistema y obtener su aprobación (ICONTEC, 2013).

La guía o herramienta del proceso sugiere estructurar el enfoque del sistema de gestión de seguridad de la información con base al análisis de riesgos y seguir la Norma 27005:2009 sobre gestión de riesgos de seguridad de la información. Es decir, el cómo hacerlo depende del tratamiento de riesgos y este, a su vez, está supeditado a los requisitos del sistema, definidos en los objetivos del SGSI. Un buen comienzo para la gestión de riesgos es la clasificación de la información y activos, la definición de vulnerabilidades, amenazas y riesgos y posterior aplicación de controles, temas introductorios vistos en la unidad 1.

» **Salida**

Como salida se obtiene un documento que describe la política de seguridad de la información que cuenta con la aprobación de la alta dirección. Este es un proceso iterativo, es decir, que requiere confirmaciones posteriores (ICONTEC, 2012).

» **Información adicional**

La Norma NTC -ISO/IEC 27005:2009 da información adicional con respecto a los criterios para la valoración de riesgos (ICONTEC, 2012).

Al realizar el proceso completo se obtiene la política de seguridad de la información. Este proceso implica la aplicación de la Guía 6 de la ISO 27003. A continuación, en la Tabla 3 se indican los numerales de la norma. La entrada, guía y salidas se encuentran en la norma:

Tabla 3. Enunciados de la Guía 6 de la Norma ISO 27003

Numeral
6.2 Definir el alcance y los límites de la organización
6.3 Definir el alcance y los límites de las Tecnologías de la Información y las Comunicaciones (TIC)
6.4 Definir el alcance y los límites físicos
6.5 Integrar cada alcance y los límites para obtener el alcance y los límites del SGS

Fuente: elaboración propia. Adaptada de ICONTEC Internacional (2012)

Para información completa, se debe consultar la norma Guía Técnica Colombiana GTC –ISO/IEC 27003.

2.1. Planes de sensibilización

Muchas personas dentro de las organizaciones desconocen las implicaciones que tiene la gestión de seguridad de la información y no comprenden completamente las políticas de seguridad implementadas.

Estudios demuestran que la mayoría de ataques provienen del interior de la organización y no de eventos externos y la causa raíz de este fenómeno se debe al desconocimiento de los usuarios finales en temas de seguridad de la información.

Por lo anterior, para una eficiente implementación de la política de seguridad de la información se requiere la aplicación de un plan o programa de sensibilización. Este es una estrategia que, por medio de herramientas didácticas y prácticas, permite a los individuos involucrarse en un tema específico para el cumplimiento de alguna ley, norma o política.

En términos de seguridad de la información, los planes de sensibilización son de vital importancia pues, como se estudió anteriormente, para implementar una política es necesario contemplar todos los aspectos de una organización. En ese sentido, la totalidad de los miembros de la empresa deben participar activamente en el cumplimiento de la política.

Para elaborar un plan de sensibilización eficaz se propone lo indicado en la Figura 1:

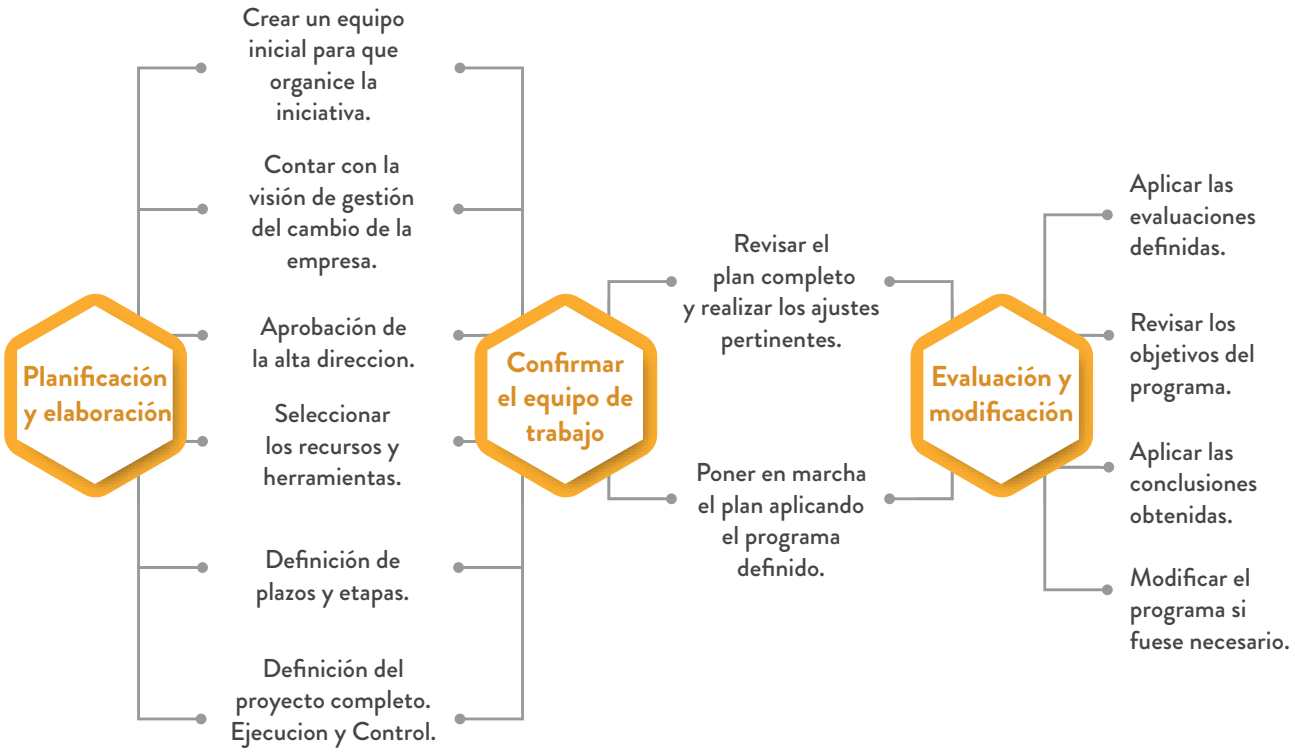

Figura 1. Fases para el diseño e implementación de un plan de sensibilización

Fuente: elaboración propia

Al igual que la política de seguridad de la información, los planes de sensibilización requieren una estructura para el cumplimiento de cada una de las fases indicadas. Dicha estructura, como mínimo, debe contener los elementos expuestos en la siguiente tabla.

Tabla 4. Estructura de un programa de sensibilización

Item de la estructura	Descripción
Introducción	Indicación general de la temática del documento donde se justifique, de manera clara, la realización del programa de sensibilización.
Objetivos	Responder a la pregunta qué se espera lograr con el plan. Se deben redactar en infinitivo de manera general.
Alineación a política	Se debe señalar cómo el programa de sensibilización se encuentra alineado con la política de seguridad. Debe incluir las políticas generales y específicas.
Alcance	Se debe indicar quiénes, cuántos individuos y cómo se verán beneficiados con el programa.
Roles y responsabilidades	Definición del equipo de trabajo con indicación de perfiles, roles y responsabilidades dentro del plan.
Metas	Orientadas a los indicadores de cumplimiento; deben ser medibles y partir de los objetivos.
Definición de audiencia	Segmentar al público objetivo con el fin de mejorar la eficiencia.
Definición de temáticas	Los temas dependen de la política y de la definición del SGSI.
Actividades de sensibilización programadas	Se deben indicar las tareas puntuales, quién las realiza, cómo lo harán y su respectiva duración.
Materiales y recursos	Son los instrumentos de sensibilización. Debe señalarse el tipo de instrumentos, el tiempo que permanecerán visibles y sus objetivos. Pueden ser afiches, folletos, protectores de pantalla, recordatorios, presentaciones, planes de capacitación.
Duración	Se debe precisar la duración completa del plan. Se propone que no sea inferior a 6 meses, dependiendo de la complejidad de la política.
Definición de evaluación	Mencionar los indicadores de calidad del programa, medios para la evaluación, frecuencia, etc.
Conclusiones	A partir de los resultados de la evaluación, se deben establecer las conclusiones sobre el programa orientadas al cumplimiento de las metas y los objetivos.
Plan de mejora	Proponer planes de mejora de acuerdo con los resultados obtenidos.

Fuente: elaboración propia

3. Seguimiento y mantenimiento de una política

El seguimiento y mantenimiento de una política depende de la definición del plan de mejora que se establezca para el sistema de gestión de seguridad de la información.

Con base en la revisión del modelo de gestión utilizado para el SGSI y el programa de sensibilización, se define el plan de seguimiento y mejora de la política.

Como ejemplo del plan de seguimiento y revisión del SGSI se debe consultar la Norma ISO 27001:2013, numeral 4.2.3 (ICONTEC, 2013). En resumen, la norma define que la organización debe cumplir con: la ejecución de procedimiento de seguimiento, revisión y controles de la política; revisiones continuas al sistema, que no solo incluyen la política, sino también los objetivos del sistema de gestión de seguridad de la información; medir qué tan eficaz son los controles; revisar continuamente la valoración de los riesgos y realizar auditorías internas del sistema.

Como se puede apreciar, lo solicitado por la norma en cuanto al seguimiento implica revisar todo el sistema. Recordemos que la política debe incluir la totalidad de las áreas y requerimientos de la organización y se apoya en las actividades solicitadas para la definición del sistema, como el establecimiento del contexto de la organización, la clasificación de los activos y el tratamiento de riesgos, entre otros.

Para el mantenimiento y mejora, la Norma ISO 27001:2013 solicita que la organización implemente rápidamente las mejoras que se han identificado, realice las acciones correctivas y preventivas como mejoras identificadas, aplicando la base de lecciones aprendidas, y comunique las acciones de mejora a todos los interesados de la organización, con el nivel de detalle suficiente para tal fin.

En otras palabras, la norma propone lo indicado en el programa de sensibilización, pero enfocado en el sistema de gestión; en este sentido, implica revisar el sistema y la política. En contraste, los planes de mejora para el programa de sensibilización están orientados exclusivamente al tema de sensibilización; la norma solicita revisar en conjunto todo el sistema, incluyendo la política y los planes de sensibilización. Por lo anterior, es esencial que los planes de mejora de los programas de sensibilización se alineen con el modelo de gestión de la organización y, por tanto, con la política (ICONTEC, 2013).

4. Ejemplo de un plan de sensibilización e indicadores de seguimiento

En esta sección se presenta un ejemplo práctico con algunos elementos que debe contener un plan de sensibilización. La construcción de este depende de la definición del sistema, la política, el nivel de aprobación de la alta dirección, etc.

En la empresa Alellot se ha implementado el sistema de gestión de seguridad de la información y se ha construido la política de seguridad de la información. Se debe hacer cumplir dicha política, por lo cual la empresa ha contratado a la agencia de publicidad Conexión total, puesto que se ha decidido que el lanzamiento será un evento social.

Este se reforzará con una plataforma virtual en la cual se probará no solo el conocimiento de los usuarios, sino que se les enviarán algunos elementos nocivos, los cuales pueden prevenir si conocen la política, como evitar el *phishing* al no ingresar al sitio que puedan reconocer como inseguro.

Tabla 5. Resumen del plan

Item de la estructura	Descripción
Introducción	El programa de sensibilización es indispensable para Alellot, pues se basa en la capacitación al usuario y revisión de sus conocimientos, no solo a nivel conceptual, sino también a nivel práctico. Por lo tanto, habrá amenazas de tipo incógnito, pero controladas por parte del área de TI y con apoyo de la agencia de publicidad. Esto con el fin de medir el aprendizaje del personal de manera lúdica.
Objetivos	Se espera generar una cultura de seguridad de la información desde lo práctico, que involucre a todo el personal, en la cual las personas se diviertan y alcancen metas.
Alineación a política	El programa se alinea con la política, que se resume en cultura de seguridad, conocimiento de los objetivos de negocio por parte de los colaboradores y educación continua, acompañada del reconocimiento por victorias tempranas alcanzadas.
Alcance	El programa incluye todas las áreas de Alellot, el cual trabaja de manera circular para contar con una visión de 360 grados de la empresa; es decir, todos están al mismo nivel, aunque en algún momento algunos lideran procesos por su rol o área de revisión. De esta manera, es incluyente y se usa la tecnología de acuerdo con las capacidades del personal.
Roles y responsabilidades	Existen tres roles y responsabilidades: • Promotores de cambio: son quienes impulsan la rueda de la seguridad a partir de su liderazgo en la empresa. • Ejecutores de cambio: son quienes, liderados por los promotores, mantienen en movimiento la rueda. • Evaluadores de cambio: son quienes validan el nivel de cumplimiento del plan en cuanto al alcance, cobertura y resultados.
Metas	Se plantean para un Nivel uno de madurez, en el que se desarrolla la capacidad de conocimiento: 1. Cantidad de personas que asisten al evento de lanzamiento. 2. Cantidad de personas que acceden a las plataformas para la capacitación. 3. *Top* 10 de errores comunes al usar las herramientas (aplicación de amenazas incógnitas).

Item de la estructura	Descripción
Definición de audiencia	El público se segmenta por las herramientas tecnológicas que utilizan; es decir, que más que el área de trabajo, prima las amenazas que tengan.
Definición de temáticas	Los temas son: 1. Seguridad para usuarios finales. 2. Protección fácil: sospechar, analizar y tomar acción. 3. ¿Ingreso a ese *link?* 4. Ojo con las redes sociales. 5. Ventajas de las copias de seguridad: persona precavida vale por dos.
Actividades de sensibilización programadas	1. Lanzamiento social del evento. 2. Capacitación en línea. 3. Amenaza incógnita. 4. Refuerzo para evitar las amenazas. 5. Jugando también se aprende.
Duración	1 año

Fuente: elaboración propia

Referencias

ICONTEC. (2012). *Guía Técnica Colombiana GTC-ISO/IEC 27003*. Bogota : Instituto Colombiano de Normas Técnicas y Certificacion.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO/IEC 27001*. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Teoría de la Seguridad

Unidad 3: Políticas de seguridad de la información

Escenario 6: Socialización, cumplimiento y revisión de una política de seguridad de la información

Autor: Alexandra Peña Daza

Asesor Pedagógico: Angie Viviana Laitón Fandiño

Diseñador gráfico: Kelly Valencia

Asistente: Alejandra Morales