Formulación de políticas de seguridad de la información

Breve descripción:

Este componente enseña a formular, implementar y gestionar políticas de seguridad de la información adaptadas a cada organización. Incluye conceptos, estructuras, redacción y objetivos claros. Aborda el diseño, aprobación, comunicación, implementación y revisión de políticas, promoviendo medidas estratégicas que protejan los activos y fortalezcan la cultura de seguridad en el entorno productivo.

Agosto de 2025

Tabla de contenido

Introducción

En el contexto actual, donde las organizaciones trabajan en entornos mediados por las tecnologías, la formulación de políticas de seguridad de la información, ha sido uno de los pilares para garantizar la protección y correcta gestión de los datos. Estas políticas no solo buscan establecer directrices para la conservación de la confidencialidad, la integridad y la disponibilidad de la información, sino que también buscan alinear las acciones de la organización con estándares normativos y mejores prácticas internacionales.

Por consiguiente, la finalidad de este componente formativo es proporcionar las bases conceptuales y procedimentales para diseñar y gestionar políticas de seguridad de la información, acordes a las características, cultura y necesidades de la organización. A través del análisis de su estructura, técnica de redacción, criterios de alineación y objetivos estratégicos, se busca desarrollar competencias para la creación de documentos claros, coherentes y efectivos que sirvan como marco de actuación frente a amenazas y riesgos.

De igual manera, se abordarán las etapas clave de la gestión de políticas, desde su diseño y aprobación, hasta la comunicación, implementación y revisión, fomentando con ello una visión integral que permita su aplicación práctica en escenarios reales. Con esto se pretende fortalecer la capacidad de respuesta de las organizaciones ante incidentes y retos de seguridad, mejorando la confianza depositada por sus clientes, empleados, aliados y demás interesados.

Partiendo de lo anterior, se invita a que acceda al siguiente video, el cual relaciona la temática a tratar durante este componente formativo:

Video 1. Fundamentos de políticas de seguridad de la información

Enlace de reproducción del video

Video 1. Síntesis del video: Formulación de políticas de seguridad de la información
En la actualidad, contar con políticas claras de seguridad de la información es indispensable para proteger los recursos estratégicos de las organizaciones y responder a las crecientes exigencias normativas y de seguridad. Este componente formativo profundiza en los fundamentos que guían la formulación de dichas políticas, abordando su concepto, estructura, técnicas de redacción y los criterios que garantizan su alineación con las características de cada institución. A lo largo del contenido, también se estudian los objetivos de seguridad de la información, entendidos como la base para orientar acciones concretas que aseguren

la confidencialidad, integridad y disponibilidad de los datos. Se explica su importancia, los requisitos que deben cumplir y la metodología más adecuada para su diseño, de modo que respondan a las necesidades y prioridades organizacionales.

Finalmente, se aborda la gestión integral de las políticas de seguridad, un proceso que incluye su diseño, aprobación, comunicación, implementación y revisión periódica. Estas etapas permiten garantizar que las políticas se mantengan vigentes, efectivas y alineadas con un ciclo de mejora continua.

Este aprendizaje ofrecerá a los aprendices una visión práctica y estratégica, orientada a fortalecer la cultura de seguridad de la información, promover el cumplimiento normativo y consolidar entornos organizacionales más seguros y confiables.

1. Políticas de seguridad de la información

Representan el pilar sobre el cual se va a definir, organizar y regular la protección de los activos de información en una organización. Las políticas no se limitan solo a ser unos documentos formales, por el contrario, representan compromisos estratégicos que guían la ruta que tiene que seguir el personal, frente a las amenazas y los riesgos. A través de ellas, se establecen los principios, los lineamientos y las responsabilidades que orientan la gestión de la seguridad, buscando que las decisiones y acciones que se tomen, estén alineadas con los objetivos organizacionales. Entender su importancia y su correcta formulación, es fundamental para fortalecer la entereza de la empresa y garantizar la continuidad del negocio en un entorno cada vez más digitalizado y expuesto a incidentes.

En este tema, se abordará el concepto, la estructura, las técnicas de redacción y los criterios para alinear las políticas de seguridad de la información con las características propias de cada organización. Además, se destacará su papel estratégico en la protección de los activos, la mitigación de los riesgos y el cumplimiento de la normativa.

1.1 Concepto

En este apartado se explorará el concepto de una política de seguridad de la información, con el fin de que puedan entender mucho mejor su propósito, alcance e importancia dentro de una organización; por ello, a continuación, se presentan diferentes definiciones formales (autores) y una más informal (propia) para facilitar su comprensión:

- **Orsys (s.f.)**

  Una política de seguridad de la información, es un documento estratégico y operativo que indica el conjunto de directrices, normas y procedimientos en los que se ampara una organización (asociación, empresa o entidad pública), con el propósito de proteger sus activos de información (datos, sistemas, infraestructura) frente a las amenazas internas y externas que se puedan tener, motivando una cultura de seguridad organizacional.

- **Función pública (2020)**

  Es una declaración general institucional definida para la protección de los activos de información, aplicando lineamientos a los procesos internos y compatibles con el modelo de gestión existente, que guía y sensibiliza sobre el uso responsable de los datos que son clasificados como críticos.

- **Fortinet (s.f.)**

  Son un conjunto de procedimientos y normas, que se han generado para dar garantías sobre el uso y el acceso seguro a los recursos y los activos de información, al personal y demás interesados. Las políticas son más que estrategias, al representar un reflejo de la cultura de la organización, donde el éxito de su implementación depende del compromiso que tengan todos los miembros de la organización.

- **Propia**

  Una política de seguridad de la información es un conjunto de reglas y acuerdos, con los cuales una empresa o una organización cualquiera, establece para cuidar la información que considere importante. Aquí se indica qué se puede hacer y qué no, sobre quién recae la responsabilidad

de proteger los activos de información y cómo se tienen que manejar para evitar su perdida, daño o acceso no autorizado; en otras palabras, es un manual que da las directrices para mantener protegida la información frente a amenazas y riesgos.

Hay que tener en cuenta que con las políticas se establecen los principios y objetivos generales de la seguridad de la información y que estas tienen que ser aprobadas por las directivas de la empresa.

Por lo que se puede entender, las políticas de seguridad de la información, son guías revestidas de mucha importancia para la protección de los recursos físicos y tecnológicos que contienen la información más relevante y cuya efectividad depende de que los miembros de la empresa las comprendan, acepten, respeten y apliquen, fortaleciendo así la cultura de seguridad y minimizando los riesgos internos y externos.

1.2 Estructura

La estructura de una política de seguridad de la información, está compuesta por una serie de lineamientos y elementos que permiten establecer un marco sólido para una efectiva protección de los activos de la información. En la siguiente tabla, se detallan los principales elementos, los cuales pueden variar según las necesidades y recursos de la organización, con una explicación, un ejemplo para una mayor comprensión y sugerencias de normativas aplicables:

Tabla 1. Lineamientos de la estructura de una política de seguridad de la información

Lineamiento	Explicación	Ejemplo para pyme	Normativa / Estándar
Propósito, objetivo y alcance.	Documenta el compromiso de la alta dirección y define para qué, a quién, dónde y cuándo aplica la política.	Una tienda de repuestos de automóviles define que su política aplica a todos los empleados, a la base de datos de clientes y proveedores y a los equipos de cómputo utilizados en la oficina y el almacén.	ISO/IEC 27001, cláusula 5.2.
Alcance, propietario y accesibilidad.	Define responsables, mecanismos de mantenimiento y de fácil acceso para todos.	El coordinador de TI es el responsable de mantener la política actualizada y accesible en intranet y restringe el uso de computadoras para fines laborales, prohibiendo	ISO/IEC 27001, cláusula 5.3.

Lineamiento	Explicación	Ejemplo para pyme	Normativa / Estándar
		instalar software sin autorización.	
Compatibilidad con políticas dependientes.	Establece como guía para políticas específicas vinculadas al SGSI.	La política general obliga a tener políticas complementarias sobre contraseñas y respaldo.	ISO/IEC 27001, Anexo A (A.5–A.18).
Roles y responsabilidades.	Se asignan los roles y las responsabilidades clave (administrador, coordinador, gerente, comité SGSG, entre otros), de forma clara y específica, para aplicar, supervisar y revisar la política,	El gerente aprueba cambios en la política, el encargado de sistemas implementa las medidas de seguridad y todos los empleados protegen sus credenciales de acceso.	ISO/IEC 27001, cláusula 5.3 (Roles, responsabilidades y autoridades).

Lineamiento	Explicación	Ejemplo para pyme	Normativa / Estándar
	asegurando así su implementación efectiva y cumplimiento.		
Excepciones y sanciones.	Permite excepciones justificadas y detalla consecuencias por incumplimientos.	En casos excepcionales, se puede autorizar el acceso remoto tras aprobación, pero el uso no autorizado puede derivar en sanciones disciplinarias.	ISO/IEC 27001, A.18 (cumplimiento). Código Sustantivo del Trabajo de Colombia.
Glosario de términos.	Se incluye un glosario de términos para ayudar al personal a entender el contenido del documento.	Se definen términos como activo, riesgo, incidente, disponibilidad, entre otros.	ISO/IEC 27001, A.7.2.2 (capacitación).

Lineamiento	Explicación	Ejemplo para pyme	Normativa / Estándar
Clasificación y control de datos.	La información es clasificada en categorías, tales como: interna, confidencial, pública. Con base en esa clasificación, se controla quiénes tienen o no acceso a ella.	La empresa clasifica la información en tres niveles: pública (catálogo de productos), interna (manuales de procedimientos) y confidencial (datos de clientes y facturación), aplicando medidas de protección según el nivel.	Ley 1581 de 2012 (Protección de datos personales) y ISO/IEC 27001, A.8.
Controles de seguridad.	Enumera medidas como contraseñas, autenticación multifactor, cifrado, redes seguras y medidas físicas para	Una empresa requiere cambiar contraseñas cada tres meses, activar el doble factor de autenticación en correos corporativos y mantener	ISO/IEC 27001, A.9 (Control de acceso) y A.12 (Seguridad en las operaciones).

Lineamiento	Explicación	Ejemplo para pyme	Normativa / Estándar
	proteger la información.	actualizados los antivirus en todos los equipos.	
Manejo de incidentes.	Establece los pasos a seguir en caso de un incidente de seguridad: detección, reporte, respuesta y recuperación.	Si un empleado detecta un correo sospechoso, debe reportarlo de inmediato al encargado de TI, quien bloqueará el acceso y revisará el sistema para prevenir daños.	ISO/IEC 27001, A.16 (Gestión de incidentes de seguridad de la información).
Revisión y actualización.	Define cuándo y cómo se revisará la política para mantenerla vigente frente a cambios	La política se revisa cada año o cuando se adquiere nueva tecnología, para adaptarse a los cambios y mejorar las	ISO/IEC 27001, cláusula 10.2 (Mejora continua).

Lineamiento	Explicación	Ejemplo para pyme	Normativa / Estándar
	organizacionales o tecnológicos.	medidas de seguridad.	

Cabe aclarar que las políticas de seguridad de la información, son un documento marco que reúne y establece la dirección general para proteger los activos informativos de la organización y que dicho marco, está compuesto por políticas específicas de seguridad, que se formulan, implementan y mantienen en la empresa, para usos concretos, tales como: el control de accesos, uso aceptable de recursos, la gestión de contraseñas o el respaldo de los datos, entre otros.

Lograr estructurar las políticas de seguridad de la información, teniendo en cuenta los principales lineamientos, permiten su comprensión por parte de todos los interesados, facilitan su implementación, aseguran su alineación con la normativa vigente y la cultura organizacional.

1.3 Técnica de redacción

Para redactar políticas de seguridad de la información, se debe garantizar un lenguaje claro, preciso, coherente y accesible a todos los miembros de la organización, independientemente de su nivel técnico. Un texto mal redactado puede generar ambigüedad, confusión o interpretaciones erróneas, lo cual afectará su correcta aplicación.

Para una buena redacción de políticas se dan las siguientes recomendaciones:

1. **Lenguaje claro y directo**

    - Evitar tecnicismos innecesarios y en caso de tener que hacerlo por el tema de la tecnología, apoyarlo con un glosario de términos.
    - Utilizar frases cortas y simples, en vez de indicaciones largas o ambiguas.
    - **Ejemplo**: en lugar de “mantener una conducta adecuada con la información”, escribir “cifrar todos los archivos clasificados como confidenciales antes de enviarlos por correo electrónico”.

2. **Estructura lógica**

    - Organizar la política en secciones bien definidas, que sigan un orden jerárquico o temático (objetivo, alcance, responsables, procedimientos, excepciones). Esto es para el marco general.
    - Facilita la lectura y comprensión, asegurando que no se omitan aspectos clave.
    - **Ejemplo**: un índice con apartados numerados (1. Objetivo, 2. Alcance, 3. Responsables) y así sucesivamente.

3. **Precisión en los términos**

    - Saber utilizar las expresiones, evitando que estas puedan dar lugar a múltiples interpretaciones.
    - Evitar palabras vagas como “adecuado” o “correcto” sin definir su significado en el contexto.

- **Ejemplo**: en vez de “proteger los datos importantes”, decir “respaldar diariamente todos los archivos clasificados como críticos en el servidor seguro de la empresa”.

4. **Consistencia**

    - Aplicar y mantener un estilo único y una terminología uniforme en las políticas y documentos relacionados. Esto evita confusiones y transmite profesionalismo.
    - **Ejemplo**: usar siempre “activo de información”, en lugar de alternar entre “activo informático” o “activo digital”, sin justificación.

5. **Enfoque en la acción**

    - Redactar en un estilo normativo, indicando en lo posible lo que se debe y no se debe hacer, así como las responsabilidades y las consecuencias.
    - **Ejemplo**: el área de TI debe revisar el registro de accesos cada 24 horas y reportar cualquier intento no autorizado.

6. **Adaptación al contexto**

    - Considerar el tamaño de la empresa, el sector y la cultura organizacional para que las políticas sean realistas y aplicables.
    - **Ejemplo**: una política de copias de seguridad para una microempresa, podría establecer respaldos semanales, mientras que para una gran empresa podrían ser cada 6 horas.

7. **Especificar responsables y destinatarios**

    - Indicar qué cargos o áreas son responsables de cumplir cada disposición.
    - **Ejemplo**: el responsable de TI deberá ejecutar copias de seguridad diarias y verificar su integridad semanalmente.

Igualmente, y no menos importante, se relaciona otra serie de recomendaciones:

01. Establecer criterios medibles y verificables

- Definir parámetros cuantitativos o plazos claros que permitan evaluar el cumplimiento.
- **Ejemplo**: actualizar los parches de seguridad en un plazo máximo de 48 horas desde su publicación oficial.

02. Mantener coherencia con la normativa vigente

- Alinear con la normatividad nacional o internacional que se exija para la empresa, según su naturaleza o actividad.
- Evitar contradicciones con reglamentos internos o leyes nacionales.
- **Ejemplo**: incluir en la política de protección de datos personales los lineamientos de la Ley 1581 de 2012.

03. Redactar en voz activa

- Usar estructuras que asignen responsabilidad directa.
- **Ejemplo**: “el jefe de seguridad debe aprobar las solicitudes de acceso”, en vez de “las solicitudes de acceso deberán ser aprobadas”.

04. Incluir ejemplos prácticos cuando sea posible

- Facilitar la comprensión, sobre todo en personal sin experiencia técnica, que, por lo general, terminan siendo los eslabones más débiles de la cadena y por donde más fácil se dan las filtraciones o fallos de seguridad.
- **Ejemplo**: en una política de uso de contraseñas, incluir una contraseña robusta y una lista de prácticas prohibidas.

05. Evitar cláusulas demasiado generales

- No redactar políticas tan amplias que no se puedan supervisar o medir.
- Si un tema es complejo, dividirlo en subpolíticas específicas.
- **Ejemplo**: separar la “política de control de acceso” de la “política de gestión de contraseñas”, en lugar de fusionarlas de forma vaga.

06. Revisar y validar antes de publicar

- Probar las políticas con un grupo reducido de empleados en la empresa, para verificar que se entiendan y que sean aplicables.
- **Ejemplo**: aplicar la política de control de accesos durante una semana en el área de contabilidad, recopilar sus observaciones y ajustar el documento antes de su aprobación oficial.

Conociendo las recomendaciones previamente dadas, a continuación, se presenta una tabla comparativa que ilustra ejemplos de políticas redactadas de forma incorrecta y correcta. De esta forma, se podrán identificar errores comunes y reconocer las prácticas adecuadas en su formulación. Su análisis servirá para facilitar la creación de políticas claras, precisas y efectivas para la organización:

Tabla 2. Políticas redactadas de forma correcta e incorrecta

No.	Política mal redactada	Política bien redactada
1	Todos los empleados deben cuidar la información.	Todos los empleados deben proteger la información de la empresa, evitando compartir datos sensibles sin autorización previa del área de seguridad de la información.
2	No se deben usar contraseñas fáciles.	Las contraseñas deberán contener al menos 12 caracteres, incluyendo mayúsculas, minúsculas, números y símbolos, además de renovarse cada 90 días.
3	El personal debe hacer copias de seguridad cuando sea necesario.	El personal del área de sistemas, deberá realizar copias de seguridad de todos los servidores críticos cada 24 horas, verificando su integridad semanalmente.
4	No se puede acceder a la información de forma indebida.	El acceso a la información clasificada, estará limitado únicamente a los usuarios autorizados, mediante credenciales asignadas por el administrador del sistema.
5	Hay que mantener segura la red.	La red corporativa, deberá estar protegida mediante firewall, segmentación de redes

No.	Política mal redactada	Política bien redactada
		y monitoreo continuo, con revisión mensual de configuraciones por el área de TI.
6	No se deben compartir archivos sin permiso.	Está prohibido compartir archivos que contengan datos personales o confidenciales, fuera de la organización, sin la aprobación escrita del responsable de seguridad de la información.
7	Los usuarios deben evitar riesgos en internet.	Los usuarios deberán abstenerse de acceder a sitios web no autorizados y reportar cualquier intento de phishing al equipo de soporte técnico en un plazo máximo de 2 horas.
8	No está permitido usar dispositivos ajenos.	Está prohibido conectar dispositivos externos no autorizados a los sistemas corporativos, cualquier excepción deberá estar documentada y aprobada por el jefe de TI.
9	Todos deben cuidar los equipos.	Todo usuario es responsable del uso y resguardo físico de su equipo asignado,

No.	Política mal redactada	Política bien redactada
		debiendo reportar cualquier daño o pérdida de inmediato al área de soporte técnico.
10	No se puede instalar software sin permiso.	La instalación de software en equipos corporativos está restringida al personal autorizado de TI y debe cumplir con la licencia correspondiente y evaluación de seguridad previa.

Una buena redacción facilita la comprensión y el cumplimiento de las políticas, asegurando que la política de seguridad de la información, no solo sea vista como un documento formal más, sino como una herramienta práctica para la protección de la información.

1.4 Criterios de alineación con características de la organización

La formulación de una política de seguridad de la información, obligatoriamente tiene que estar alineada con las particularidades, objetivos y cultura de la organización, para asegurar su eficacia y aceptación. Esto implica que el marco general no debe ser un documento genérico, mucho menos que las políticas de una empresa pueden ajustarse como un molde en otra empresa; por lo tanto, hay que considerar diferentes aspectos como el sector productivo, el tamaño de la empresa, su estructura organizativa, el nivel de actualización tecnológica y la normativa aplicable en su contexto.

Dentro de los criterios que se pueden tener en cuenta para lograr una buena alineación, se indican los siguientes:

- **Coherencia con la misión, visión y valores corporativos**

  La política debe reflejar y apoyar la razón de ser de la organización, promoviendo procedimientos y comportamientos que respalden su filosofía empresarial.

  Ejemplo: una empresa agropecuaria, con enfoque en sostenibilidad, debe integrar en su política, prácticas de protección de datos que minimicen el uso de papel y prioricen medios digitales seguros.

- **Adaptación a la estructura y roles internos**

  Las disposiciones tienen que considerar lo que son la jerarquía, las responsabilidades y funciones, en las diferentes áreas, con el fin de facilitar su implementación y control.

  Ejemplo: si el área de ventas trabaja de forma remota, la política debe incluir medidas específicas de acceso seguro a la información desde dispositivos móviles.

- **Adecuación a recursos y capacidades disponibles**

  Se tiene que contemplar una infraestructura tecnológica, un presupuesto, un nivel de capacitación del personal que labora en la empresa y unas herramientas existentes, pero hay que tener en cuenta que no se pueden hacer exigencias que se consideren inalcanzables.

Ejemplo: en una pyme sin equipo de TI dedicado, se pueden establecer revisiones de seguridad trimestrales en lugar de mensuales, siempre que no se comprometa la protección de la información.

- **Cumplimiento normativo y sectorial**

  Las políticas tienen que ajustarse a la legislación nacional y a la internacional, siempre y cuando apliquen al sector de desempeño de la empresa; así como a las certificaciones y estándares que la empresa esté adoptando o piense adoptar.

  Ejemplo: una organización que procese datos personales de clientes, debe garantizar el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios en Colombia.

- **Compatibilidad con la cultura organizacional**

  Tanto la política de seguridad de la información con marco normativo, como las políticas específicas que la conforman, tienen que ser entendibles y aceptadas por todo el personal; por lo tanto, se tiene que evitar un lenguaje excesivamente técnico, para que fomente la participación y el compromiso dentro de la organización.

  Ejemplo: incluir talleres prácticos y simulaciones para que todos los empleados comprendan y adopten los lineamientos establecidos.

La formulación de políticas de seguridad de la información, constituye una columna vertebral para garantizar la protección de los activos de información y el cumplimiento de los objetivos estratégicos de la organización. Una política de seguridad de la información en singular, es el documento o marco rector que define la visión, el

alcance y los lineamientos generales que guían la gestión de la seguridad en toda la empresa; mientras que las políticas de seguridad de la información en plural, son los documentos específicos que desarrollan y aplican los lineamientos a diferentes áreas o procesos, como el control de accesos, la gestión de contraseñas o el uso aceptable de dispositivos, entre otras; que a su vez están conformadas por un listado de políticas o subpolíticas. Aunque al inicio pueda existir confusión, con la práctica esta se disipa por completo.

Comprender estas distinciones, es imperativo para evitar confusiones y lograr que la estrategia de seguridad sea coherente y efectiva. Solo con una política general sólida, respaldada por políticas específicas bien diseñadas y alineadas con la organización, será posible fomentar una cultura de seguridad, minimizar los riesgos, proteger los activos de información y responder de forma proactiva a las amenazas que se enfrentan en el entorno empresarial.

2. Objetivos de seguridad de la información

Son la guía estratégica para proteger los activos más valiosos de una organización, frente a amenazas y riesgos. En este tema, se abordará su concepto, importancia, requisitos esenciales y la metodología para diseñarlos de manera efectiva. El propósito es comprender cómo estos objetivos fortalecen la confianza en las organizaciones.

2.1 Concepto

A continuación, se presentan dos conceptos sobre los objetivos de seguridad de la información, con el fin de que comprendan su significado desde la parte técnica y general; con ello, se puede tener una mejor idea al respecto:

- **Definición técnica**

  Los objetivos de seguridad de la información son las metas que una empresa define para proteger sus activos de información, frente a los riesgos identificados. Los objetivos definidos tienen que ser coherentes con la política de seguridad, medibles, estar alineados con el tratamiento de los riesgos, comunicados y actualizables en la medida que se vayan dando cambios en el entorno; además, la empresa tiene que documentarlos y planificar quién los alcanzará, con qué tipo de recursos, en qué plazo y cómo se evaluará su cumplimiento (EEE, 2022).

- **Definición general**

  Un objetivo de seguridad de la información es una meta que busca garantizar en una organización la protección de sus activos de información

más valiosos y de sus sistemas, frente a las amenazas y riesgos. Estos direccionan las acciones y los controles que se necesitan para conservar la confidencialidad, integridad y disponibilidad de la información. También sirven como referencia para evaluar el desempeño de las medidas que se implementan y promueven con el fin de mantener una mejora continua. Para tener éxitos con ellos en las empresas, los objetivos tienen que ser claros, medibles y realistas, de tal forma que puedan irse adaptando a los diversos cambios tecnológicos, logísticos, empresariales y de la dinámica del entorno, que se van dando en el tiempo.

Para que se tengan unos modelos que sirvan de guía, a continuación, se comparte una lista de ejemplos de objetivos, con una breve explicación de cada uno, de acuerdo a lo expresado por la Escuela Europea de Excelencia (EEE) (2022):

Tabla 3. Ejemplos de objetivos de seguridad de la información

Objetivos	**Descripción breve**
Reducir en un 50 % las incidencias de seguridad de la información en un plazo definido.	Busca minimizar los incidentes relacionados con accesos no autorizados, fugas de datos o mal uso de la información, mediante controles y medidas preventivas.
Cumplir al 100 % con los requisitos establecidos en la norma ISO 27001.	Garantiza que la organización implemente y mantenga todas las

Objetivos	Descripción breve
	prácticas y controles exigidos por este estándar internacional.
Atender plenamente las necesidades y expectativas del área de gestión de riesgos.	Alinea las acciones de seguridad con las políticas y criterios establecidos por el equipo responsable de identificar y gestionar riesgos.
Lograr un nivel específico de madurez en seguridad de la información.	Implica alcanzar un grado de protección definido, medido por estándares internos o externos, que permita operar de forma segura.
Obtener una certificación o acreditación oficial en seguridad de la información.	Busca que la organización sea reconocida formalmente por cumplir con altos estándares en la protección de datos y sistemas.

Conocer diferentes enfoques, facilita el conectarse con una visión más completa, lo que ayuda a interpretar y aplicar los objetivos de una mejor manera; esto, con el fin de lograr lo que se busca con ellos, que es proteger la información y fortalecer la confianza organizacional.

2.2 Importancia

La importancia de los objetivos de seguridad de la información, radica principalmente en que se convierten en la guía o la hoja de ruta que marca el rumbo para la protección de los activos de información más valiosos para una organización o empresa. Su correcta formulación, permite alinear la seguridad con las estrategias del negocio, con lo que garantizan la confidencialidad, integridad y disponibilidad de los datos.

La aplicación adecuada de estos objetivos, ayuda a aplicar los siguientes procesos:

- **Mitigación**

  Unos objetivos bien formulados, permiten priorizar recursos, definir controles adecuados, cumplir con normativa ajustada vigente y reducir la probabilidad e impacto de los incidentes.

- **Confianza**

  En todos los interesados, tales como los clientes, los aliados estratégicos, los empleados y el resto de todas las partes interesadas, demostrando con ello el compromiso que tiene la empresa con la gestión responsable de la información.

- **Prevención**

  Otro de los puntos más considerables por lo que unos buenos objetivos adquieren alta relevancia, es porque ayudan en la prevención de pérdidas económicas, daños a la reputación y sobre todo problemas legales, lo que

facilita la continuidad del negocio y fortalece su competitividad en un entorno donde la tecnología y la globalización toma cada día mayor protagonismo.

Para seguir entendiendo la importancia que revisten los objetivos y por qué se tienen que redactar muy bien, al centrar en ellos la seguridad de la información de la empresa, a continuación, se comparten unos puntos considerables con ejemplos que se toman desde la realidad de las pymes colombianas:

- **Prevención de incidentes**

  Definir objetivos claros reduce la probabilidad de ataques cibernéticos, fugas de información o errores humanos.

  Ejemplo: implementar un objetivo para que el 100 % de los empleados cambien sus contraseñas cada 90 días puede disminuir accesos indebidos.

- **Cumplimiento normativo**

  Facilitan la adaptación a leyes como la Ley 1581 de 2012 (protección de datos personales) o estándares como ISO/IEC 27001.

  Ejemplo: tener un objetivo de cumplir al 100 % con la Ley 1581 evita sanciones de la Superintendencia de Industria y Comercio.

- **Alineación con la gestión de riesgos**

  Permiten que la seguridad de la información esté integrada con el plan de gestión de riesgos de la empresa.

  Ejemplo: si el área de riesgos detecta que el acceso físico a los servidores no está controlado, un objetivo puede ser instalar cerraduras electrónicas en 30 días.

- **Mejora continua**

  Los objetivos sirven como indicadores que permiten medir y mejorar continuamente los procesos de seguridad.

  Ejemplo: reducir las incidencias de malware en un 60 % mediante campañas internas de concientización.

- **Reputación y confianza**

  Cumplir objetivos de seguridad refuerza la imagen de la empresa y la confianza de clientes y socios.

  Ejemplo: garantizar la protección de datos en operaciones en línea, ayuda a ganar la confianza de nuevos clientes.

Los objetivos de seguridad de la información, se pueden considerar piezas fundamentales para la orientación de acciones de protección de la información y sistemas de una organización, para garantizar que se mantengan alineados con la estrategia y necesidades del negocio.

2.3 Requisitos

Para formular unos adecuados objetivos, es imprescindible tener en cuenta unos requisitos, tal como lo establece la norma ISO/IEC 27001. En ella se explican en qué consisten, cómo pueden aplicarse en la práctica y se apoyan con unos ejemplos, pensando en el escenario de una pyme.

Por lo anterior, la siguiente información basada en lo expuesto por ESGinnova (s.f.), permitirá comprender no solo qué exige la norma, sino cómo puede llevarse a cabo en la realidad de forma efectiva y medible:

Tabla 4. Lista de requisitos

Requisito	Descripción	Ejemplo práctico en una pyme
Coherencia con la política de seguridad de la información.	Los objetivos tienen que alinearse con lo que se establezca en la política general de seguridad de la organización, con el fin de garantizar el respaldo institucional.	Si la política indica (proteger la información confidencial de los clientes), un objetivo podría ser (implementar cifrado en el 100 % de las bases de datos antes de fin de año).
Medible en lo posible.	Siempre que se tenga la posibilidad, los objetivos tienen que incluir indicadores que permitan evaluar su cumplimiento, ya sea de forma cuantitativa o cualitativa.	Reducir en un 30 % el número de incidentes de phishing reportados en seis meses.
Consideración de requisitos y resultados de la gestión de riesgos.	Hay que tener en cuenta las leyes, las regulaciones, los requisitos contractuales y los hallazgos que se han hayan	Establecer controles de acceso basados en roles, debido a que el análisis de riesgos detectó accesos no

Requisito	Descripción	Ejemplo práctico en una pyme
	encontrado en la evaluación de los riesgos.	autorizados como amenaza prioritaria.
Monitoreo.	Los objetivos tienen que estarse revisando periódicamente, con el fin de que se puedan verificar sus avances, posibles estancamientos o si se han dado desviaciones que no han permitido cumplir o entenderlos. Esto juega mucho con la mejora continua y también sirve para saber si tienen que ser reajustados o reformulados.	Revisar trimestralmente el porcentaje de cumplimiento de copias de seguridad realizadas, según el plan establecido.
Comunicación.	Los objetivos y su estado de avance tienen que ser comunicados a las partes interesadas, con el fin de	Presentar en la reunión mensual de gerencia el avance de los objetivos de seguridad y las acciones pendientes.

Requisito	Descripción	Ejemplo práctico en una pyme
	asegurar su comprensión y compromiso para cumplirse.	
Actualización.	Los objetivos tienen que revisarse y reajustarse cuando se den cambios en los riesgos, en el entorno o en las prioridades de la empresa.	Actualizar el objetivo de seguridad para incluir la protección de información en los teléfonos celulares, para quienes se han ido a trabajar de forma remota en campo.
Disponibilidad como información documentada.	Los objetivos tienen que registrarse formalmente y estar disponibles como parte de la documentación de un SGSI.	Guardar en el repositorio de la empresa un documento actualizado con todos los objetivos de seguridad, fechas y los responsables.
Planificación detallada para lograrlos.	Se debe definir qué se hará, qué recursos se usarán, quién será responsable, los plazos y los criterios de evaluación.	Plan para implantar autenticación multifactor en todos los sistemas: asignar responsable del área de TI, presupuesto

Requisito	Descripción	Ejemplo práctico en una pyme
		para licencias, fecha de ejecución y auditoría final para validar cumplimiento.

Ceñirse a estos requisitos, garantiza que los objetivos formulados en su mayoría sean claros, medibles, alcanzables y que estén alineados con la cultura organizacional de la empresa. Tenerlos en cuenta y trabajar con ellos, no solo demuestra conformidad con estándares internacionales como la ISO/IEC 27001, sino que da facilidades para su seguimiento y para mantener una mejora continua, demostrando que los objetivos terminan convertidos en herramientas confiables y efectivas para proteger los activos de información de la empresa y responder oportunamente ante los riesgos que puedan encontrarse en el camino.

2.4 Metodología de diseño

El diseño de objetivos, requiere un enfoque sistemático que asegure su alineación con la cultura organizacional y con la normativa vigente; por lo tanto, una metodología bien estructurada ayuda en la construcción de objetivos claros, medibles y sobre todo realistas, garantizando su evaluación y mejora continua. Se recomienda tener en cuenta las siguientes directrices para trabajar en la construcción de los objetivos:

1. **Análisis del contexto organizacional**

   Aquí se recomienda identificar el tipo de información que se maneja, los riesgos y las amenazas, los requisitos legales y la normativa aplicable.
   Ejemplo: la empresa maneja datos sobre producción, ventas y salud del ganado y debe cumplir con la Ley 1581 de 2012 sobre protección de datos.

2. **Alineación con la política de seguridad de la información**

   Se asegura que los objetivos respalden los principios y directrices establecidos en la política general de la organización.
   Ejemplo: si la política establece (proteger la información crítica de la empresa), un objetivo podría ser: implementar un sistema de copias de seguridad semanal.

3. **Definición de objetivos SMART**

   Los objetivos deben ser específicos, medibles, alcanzables, relevantes y con un tiempo definido. Más adelante se profundizará en esta técnica, la cual es recomendable para la construcción de los objetivos.
   Ejemplo: reducir en un 30 % los incidentes de pérdida de datos en 12 meses.

4. **Asignación de responsables y recursos**

   Se determina quién liderará cada objetivo y qué recursos (humanos, tecnológicos, financieros) serán los necesarios para ello.
   Ejemplo: el jefe de TI será responsable de la implementación del control de accesos.

5. **Plan de seguimiento y evaluación**

   En esta parte se establecen indicadores y métodos para medir el avance y cumplimiento de los objetivos.

   Ejemplo: indicador: número de incidentes de acceso no autorizado detectados mensualmente.

6. **Revisión y mejora continua**

   En esta etapa final, es donde se ajustan los objetivos en función de cambios en el contexto, resultados de evaluaciones y auditorías internas.

   Ejemplo: revisar los objetivos cada seis meses para adaptarlos a nuevas amenazas tecnológicas.

Una de las metodologías más usadas en la construcción de objetivos es la SMART, cuyo nombre parte de un acrónimo por sus siglas en inglés, por alinearse con todas las especificaciones y necesidades de los objetivos de seguridad de información en una organización.

Dicha metodología, se explica a continuación:

Específico (specific)

S – El objetivo debe estar claramente definido, sin ambigüedades, indicando qué se quiere lograr, quién será responsable y sobre qué información o proceso se trabajará.

Ejemplo: implementar un sistema de respaldo semanal de la base de datos de inventario del ganado.

Medible (measurable)

M – Incluye indicadores cuantitativos o cualitativos que permitan evaluar el progreso y el grado de cumplimiento.

Ejemplo: reducir en un 30 % los incidentes de pérdida de datos en 6 meses, medido por el registro de incidentes mensuales.

Alcanzable (achievable)

A – El objetivo debe ser realista, considerando los recursos humanos, técnicos y financieros de la organización.

Ejemplo: capacitar al 100 % del personal administrativo en manejo seguro de contraseñas en un plazo de 3 meses, utilizando el presupuesto actual de capacitación.

Relevante – (relevant)

R – Tiene que alinearse con las prioridades estratégicas de la organización y aportar valor real a la seguridad de la información.

Ejemplo: proteger la información de trazabilidad del ganado para cumplir con requisitos legales y de exportación.

Limitado en el tiempo – (time bound)

T – Definir un plazo para su cumplimiento, lo que ayuda a priorizar y planificar las acciones.

Ejemplo: implementar un sistema de control de accesos físicos en la oficina administrativa antes del 30 de junio de este año.

Para mayor comprensión, a continuación, se comparten nuevos ejemplos de objetivos de seguridad de la información, utilizando la técnica SMART, aplicada a diferentes sectores pyme:

1. **Empresa de consultoría contable**

   Reducir en un 30 % los incidentes de phishing detectados en la empresa, mediante capacitaciones mensuales al personal durante los próximos 6 meses.

2. **Agencia de marketing digital**

   Implementar un sistema de copias de seguridad automáticas en la nube para todos los equipos de la empresa, antes del 15 de diciembre, con verificación semanal de su correcto funcionamiento.

3. **Empresa de desarrollo de software**

Disminuir en un 25 % los tiempos de respuesta ante incidentes de seguridad, mediante la creación y aplicación de un protocolo de actuación antes de 4 meses.

4. **Firma de abogados**

   Lograr que el 100 % de los empleados firmen y comprendan la política de seguridad de la información, antes del 31 de marzo, con sesiones explicativas de 1 hora para cada área.

5. **Empresa de comercio electrónico**

   Reducir en un 40 % el número de contraseñas débiles detectadas, mediante la implementación de autenticación multifactor en todos los accesos críticos en un plazo de 3 meses.

6. **Empresa de logística**

   Aumentar en un 50 % la detección temprana de amenazas internas, mediante la instalación de un software de monitoreo de actividad antes del final del trimestre.

7. **Clínica odontológica**

   Capacitar al 90 % del personal en manejo seguro de datos personales en un programa de formación de 2 horas, antes del 30 de junio.

8. **Empresa de impresión y diseño gráfico**

   Reducir las vulnerabilidades críticas identificadas en auditorías internas en un 70 % en los próximos 5 meses, mediante la aplicación de parches y actualizaciones.

9. **Empresa de consultoría tecnológica**

   Conseguir la certificación ISO 27001 en un periodo de 12 meses, para reforzar la confianza de los clientes y socios estratégicos.

10. **Empresa de arquitectura e ingeniería**

    Disminuir en un 35 % el acceso no autorizado a archivos sensibles, mediante la implementación de permisos basados en roles en un plazo de 4 meses.

La formulación de objetivos de seguridad de la información bajo la metodología SMART, permite a las pymes establecer metas claras, medibles y alcanzables, alineadas con su realidad operativa y recursos disponibles. Este enfoque no solo facilita el seguimiento y la evaluación de avances, sino que también garantiza que las acciones estén orientadas a resultados concretos y relevantes para la protección de los activos de información.

Además, al definir plazos precisos, se fomenta la disciplina y el compromiso organizacional para cumplir con las metas propuestas, fortaleciendo así la cultura de seguridad en la empresa.

3. Gestión de riesgo

Esta gestión barca el conjunto de acciones que son necesarias para que se pueda garantizar unas políticas bien diseñadas, aprobadas, comunicadas, implementadas y revisadas de forma efectiva. Gracias a este proceso, las directrices establecidas, pueden mantenerse alineadas con las necesidades de la organización y los cambios del entorno, asegurando así su vigencia y aplicabilidad en el tiempo. En esta temática, se analizará que puntos clave pueden conformar esta gestión, proporcionando pautas para una correcta aplicación en las organizaciones.

3.1 Concepto

La gestión de políticas de seguridad de la información, hace referencia al proceso sistemático que se trabaja para que una organización planifique, desarrolle, implemente, supervise y actualice sus políticas, con la finalidad de proteger sus activos de información. Este proceso garantiza que las políticas a parte de cumplir con la normativa base y estándares adoptados, también respondan a las necesidades reales de organización, de tal forma que se puedan ir aplicando y adaptando a los cambios tecnológicos, operativos y de riesgos. El realizar un trabajo de forma correcta y bien aplicada, facilita que las políticas sean comprendidas, aceptadas y aplicadas por todos los miembros de la organización y el resto de las partes interesadas, fortaleciendo así la cultura de seguridad de la organización.

3.2 Diseño

El diseño de una política de seguridad de la información, debe ser intencional y adaptarse al contexto de la organización. Según la norma ISO/IEC 27001, la alta dirección tiene la responsabilidad de asegurar que la política se ajuste al propósito de la

organización, incluya los objetivos de seguridad, refleje el compromiso de mejora continua y, sobre todo, cumpla con los requisitos aplicables. De igual manera, la norma ISO/IEC 27002, establece que estas políticas específicas, tienen que estar bien definidas, redactadas de manera formal, contar con la aprobación de las directivas, comunicarse eficazmente con el personal responsable o al que corresponda y someterse a revisiones periódicas en periodos planificados (Morgan Hill, s.f.).

El diseño tiene que incluir componentes claros como el propósito, el alcance, los roles y las responsabilidades; además de los fundamentos que justifican su existencia. No se puede olvidar, que tiene que equilibrarse la seguridad con la productividad, involucrando a los actores clave y estar documentada para facilitar su aplicación práctica.

Aunque ya se ha mencionado la relevancia de las políticas de seguridad de la información, en este punto se retoma el tema desde la perspectiva de la ISO/IEC 27002. No basta con reconocer qué es una política y su función dentro del SGSI, ya que resulta imprescindible comprender los pasos formales que aseguran su adecuada definición, aprobación, comunicación y revisión, de manera que se garantice una correcta implementación alineada con las necesidades organizativas.

Es por ello, que en este apartado se profundiza en la aplicación práctica y normativa que orienta el diseño de políticas, destacando no solo su formulación, sino también los mecanismos para mantenerlas actualizadas y efectivas, frente a los cambios del entorno y los riesgos emergentes, lo que refuerza su papel estratégico dentro de la gestión de seguridad de la información.

3.3 Aprobación

El proceso de aprobación formal de las políticas de seguridad, es indispensable para darles legalidad, coherencia estratégica y respaldo institucional; por ello, según el ítem Control 5.1 de la ISO/IEC 27001, las políticas generales deben estar definidas y aprobadas por la alta dirección o quien haga sus veces (CYBERZONI, s.f.). Esta aprobación demuestra el compromiso que tiene la empresa con la seguridad y establece una base sólida para su gestión.

Cuando se habla de las políticas específicas por área, como control de accesos, respaldo o uso aceptable, ISO permite que estas no tengan que ser aprobadas necesariamente por la alta dirección, sino que por el contrario, estas aprobaciones pueden darse por niveles administrativos con menor relevancia, como por citar al jefe de área o el director de algún departamento en particular, siempre que sea competente y cuente con autoridad para ello (Parker, s.f.), lo que facilita una implementación más ágil y alineada con la estructura organizacional.

Para entender mejor los procesos de aprobación, se relacionan algunos ejemplos:

- **Política general de seguridad de la información**

  Aprobada por el gerente general o director ejecutivo, para asegurar respaldo institucional.

- **Política de control de acceso físico**

  Aprobada por el jefe de operaciones, responsable de los accesos a las áreas administrativas.

- **Política de uso aceptable de dispositivos**

  Revisada y aprobada por el jefe de tecnología o responsable de TIC.

Este enfoque escalonado permite distribuir responsabilidades de manera lógica, agiliza la gestión de políticas y garantiza que cada una tenga el respaldo adecuado, según su impacto en la organización.

A continuación, se relacionan unos pasos que pueden mostrar una ruta de cómo podría desarrollarse el proceso de aprobación de políticas:

1. **Redacción inicial**

   El equipo de seguridad de la información (o un comité designado) redacta el borrador de la política siguiendo las directrices de la política general.

2. **Revisión técnica**

   Especialistas del área revisan el contenido para asegurar que sea realista y aplicable. Por ejemplo, el jefe de TI revisa una política de control de acceso para confirmar que los métodos de autenticación sean viables.

3. **Ajustes y validación interna**

   Se incorporan observaciones de áreas como gestión de riesgos, legal o recursos humanos.

4. **Presentación a la alta dirección**

   El responsable de seguridad presenta el documento, justificando la necesidad de la política, el impacto esperado y los recursos que se requerirán para su aplicación.

5. **Aprobación formal**

   La alta dirección firma o registra en acta su aprobación. Esto puede quedar documentado en un repositorio oficial o en un sistema de gestión documental.

6. **Registro y control de versiones**

   La política aprobada recibe un número de versión, fecha de entrada en vigor y fecha de revisión programada.

Como complemento de lo explicado, se detallan en unos ejemplos hipotéticos en el sector pyme, por medio de casos:

Tabla 5. Ejemplos de procesos de aprobación de políticas de seguridad de la información

Caso 1 - Clínica Odontológica SONRISA PLUS	**Caso 1 - Clínica Odontológica SONRISA PLUS**
Necesidad	**Proceso de aprobación**
Durante una auditoría interna, el consultorio detecta que las historias clínicas de los pacientes se almacenan en carpetas sin control de acceso, lo que expone datos sensibles protegidos por la Ley 1581 de 2012.	**1. Identificación**: el jefe administrativo reporta a la gerencia el riesgo de incumplir la normativa de protección de datos personales. **2. Redacción**: el encargado de TI redacta una política de protección de datos y acceso a historias clínicas, estableciendo el uso obligatorio de contraseñas seguras en

	el software odontológico y acceso restringido a personal autorizado. **3. Revisión técnica y legal**: el área legal revisa que la política cumpla con la Ley 1581 y la Resolución 1995 de 1999 (historias clínicas). **4. Presentación a la gerencia**: el responsable de TI expone el borrador en la reunión mensual de gerencia. **5. Aprobación**: la gerencia aprueba la política y fija su entrada en vigor para el mes siguiente, dejando registro en acta firmada.
Caso 2 – Corporación Educativa Gabriel García Márquez	**Caso 2 – Corporación Educativa Gabriel García Márquez**

Necesidad	Proceso de aprobación
La institución identifica que los docentes usan cuentas de correo personales para enviar y recibir información confidencial de estudiantes, lo que pone en riesgo la integridad y confidencialidad de la información académica.	**1. Identificación**: el coordinador académico informa al comité de seguridad de la información sobre incidentes de filtración de datos por el uso de correos personales. **2. Redacción**: el comité elabora una política de uso de correo institucional, que establece la obligación de usar únicamente cuentas con dominio corporativo y autenticación en dos pasos. **3. Revisión técnica**: el área de TI valida la viabilidad de implementar autenticación reforzada. **4. Revisión directiva**: el consejo directivo revisa la política y propone incluir sanciones disciplinarias por incumplimiento. **5. Aprobación**: el consejo aprueba la política en sesión formal y ordena su difusión a todo el personal docente y administrativo.
Caso 3 – Supermercado MerkExpress	**Caso 3 – Supermercado MerkExpress**

Necesidad	Proceso de aprobación
Se detecta que varias computadoras del área de cajas tienen contraseñas genéricas como 12345 y que no se han cambiado en más de un año, aumentando el riesgo de accesos no autorizados al sistema de ventas e inventario.	**1. Identificación**: el jefe de caja informa al administrador general sobre el riesgo de fraude interno y pérdida de información. **2. Redacción**: el encargado de TI redacta una política de gestión de contraseñas, con reglas para longitud mínima, complejidad y cambios cada 90 días. **3. Prueba piloto**: se implementa en dos cajas por una semana para evaluar el impacto operativo. **4. Revisión gerencial**: el administrador revisa los resultados y confirma que no afecta la velocidad de atención al cliente. **5. Aprobación**: el propietario del supermercado aprueba la política, firma el documento y ordena su aplicación inmediata en todos los equipos.

La aprobación de políticas de seguridad de la información, representa un paso clave para que se pueda garantizar la legalidad y el cumplimiento de ellas, al interior de cualquier organización. Este proceso, que va desde la detección de la necesidad hasta la

validación formal, asegura que las medidas adoptadas respondan a riesgos reales, cuenten con respaldo directivo y sean aplicables de forma efectiva en la empresa.

3.4 Comunicación

La comunicación de las políticas de seguridad de la información, es el proceso que garantiza que todas las personas que trabajan en una empresa y las que tienen relación con ella, sepan cuáles son las reglas y procedimientos para proteger la información. No basta con que las políticas existan y que estén escritas en un documento, es necesario que estas sean explicadas de forma clara, sencilla y en el momento adecuado, con el fin de que todas las partes interesadas puedan comprenderlas y aplicarlas en su trabajo cotidiano. Esto lo reiteran la ISO/IEC 27001:2022 (cláusula 7.4) y las guías prácticas de ISO/IEC 27002:2022.

En este caso, comunicar establece qué se va a comunicar, a quién, cuándo, cómo y quién será el responsable de hacerlo. Por ejemplo, en una pyme pueden realizarse diversas actividades para ello, tales como reuniones, capacitaciones, carteleras, correos electrónicos, videos e incluso, charlas cortas. Hay que tener en cuenta que el lenguaje que se utiliza para comunicar, tiene que ser acorde al perfil de los empleados, por lo que, para el éxito de dicha tarea, hay que evitar tecnicismos excesivos, los cuales la mayoría de las veces dificultan la comprensión de los interesados.

Tampoco hay que olvidar y más bien toca recalcarlo, que para que la tarea de comunicar sea efectiva, no hay que limitarse solo a la entrega del documento, sino que hay que incluir la retroalimentación y la verificación de que los empleados hayan comprendido las políticas y les haya quedado claro qué repercusiones puede tener su incumplimiento en ellos. En la realidad, una empresa que logra comunicar bien sus

políticas, reduce incidentes de seguridad por desconocimiento y aumenta la participación activa de su personal en la protección de la información.

A continuación, se muestran diferentes métodos para comunicar políticas de seguridad y ejemplos que los relacionan en una pyme, los cuales se pueden utilizar según el escenario:

- **Reuniones presenciales**

  Encuentros cara a cara para explicar las políticas y resolver dudas.
  Ejemplo: la empresa convoca a todo el equipo a una reunión mensual para repasar las políticas y presentar actualizaciones.

- **Capacitaciones formales**

  Cursos o talleres estructurados para enseñar de forma detallada el contenido de las políticas.
  Ejemplo: la empresa organiza una capacitación trimestral sobre el manejo seguro de datos de pacientes.

- **Correos electrónicos internos**

  Envío de mensajes claros con el contenido o resumen de las políticas.
  Ejemplo: un supermercado envía un correo a sus 40 empleados con un archivo PDF que resume la política y ejemplos prácticos de aplicación.

- **Carteleras o señalización**

  Colocar avisos en lugares visibles para recordar las políticas.
  Ejemplo: una consultora imprime afiches con recordatorios sobre el uso seguro de contraseñas y los coloca en el área de personal.

- **Intranet o plataforma interna**

  Publicación de las políticas en un espacio digital de acceso común.

  Ejemplo: una empresa de software sube todas las políticas a su intranet y envía un enlace a los empleados.

- **Videos cortos**

  Material audiovisual que explica las políticas de forma sencilla y atractiva.
  Ejemplo: una distribuidora de ropa crea un video animado de 3 minutos que explica cómo prevenir el robo de información de clientes.

- **Charlas rápidas**

  Breves espacios de 5 a 10 minutos para recordar puntos clave.
  Ejemplo: en una distribuidora de medicamentos, antes de abrir, el encargado dedica 5 minutos a recordar la política de seguridad en el uso de datos de proveedores y clientes.

3.5 Proceso de implementación

La implementación no se limita a la distribución de un documento; por el contrario, conlleva una serie de acciones planificadas que aseguren que lo dispuesto en el documento se aplique y se cumpla de manera efectiva en la organización. Según la norma ISO/IEC 27001:2022, después de la aprobación, se tienen que establecer mecanismos que garanticen su comunicación, capacitación, aplicación, seguimiento y mejora continua.

A continuación, se detalla este proceso:

1. El proceso inicia con la planificación, allí se definen los recursos, responsables y el cronograma de ejecución.
2. Luego sigue la comunicación y la socialización, lo cual puede incluir según las directrices de la empresa, capacitaciones, guías, reuniones, afiches o señalizaciones, entre otros.
3. Acto seguido, se pone en marcha la puesta en práctica, asegurando que los controles y demás medidas que están en la política sean integradas a los procesos diarios.

   Es importante definir y mantener un sistema de seguimiento y medición, con indicadores claros que permitan evaluar el nivel de cumplimiento e identificar brechas o incumplimientos.
4. Por último, los resultados de este monitoreo alimentan el proceso de revisión y mejora, donde se revisa si se tienen que hacer ajustes a la política o a los procedimientos que cambian según el contexto, como nuevas amenazas o incidentes que han ocurrido después de implementada la política.

Basado en lo anterior, a continuación, se detallan ejemplos que muestran hipotéticamente como se pueden dar dos implementaciones:

Ejemplo 1. Empresa agropecuaria El Buen Potrero

1. **Planificación**
   - El gerente y el encargado de TI definen un plan para implementar la política de seguridad de la información, asignando un presupuesto básico para capacitación y controles físicos.
   - Se identifican los recursos: cerraduras para áreas críticas, software de gestión de datos de animales y protocolos de copia de seguridad semanal.
2. **Comunicación y socialización**
   - Reuniones cortas con todo el personal (vaqueros, veterinarios, administrativos), para explicar la importancia de proteger datos como registros de producción, inventarios y clientes.
   - Carteles en las oficinas con recordatorios sobre contraseñas seguras y manejo de información sensible.
3. **Puesta en práctica**
   - Instalación de controles de acceso físico a oficinas y bodega de medicamentos.
   - Configuración de permisos en el software para que solo el personal autorizado pueda modificar datos críticos.
4. **Seguimiento y medición**
   - Cada mes, el encargado revisa el historial de accesos físicos y digitales para detectar anomalías.
   - Reporte trimestral al gerente sobre incidentes o mejoras necesarias.
5. **Revisión y mejora**

- Ajustes a los protocolos luego de detectar que los backups no estaban siendo verificados.
- Inclusión de capacitación anual obligatoria sobre manejo seguro de información.

Ejemplo 2: Empresa de desarrollo de software PANAMSOFT

1. **Planificación**
   - El director de proyectos y el oficial de seguridad de la información (CISO), elaboran un plan para implementar la política en los equipos de desarrollo y soporte.
   - Se definen recursos: herramientas de gestión de control de versiones seguras, capacitación en OWASP, y VPN para acceso remoto seguro.
2. **Comunicación y socialización**
   - Taller inicial para todo el personal explicando riesgos como fuga de código fuente, robo de credenciales o malware.
   - Publicación de un manual interno en la intranet sobre buenas prácticas de seguridad.
3. **Puesta en práctica**
   - Implementación de autenticación multifactor para el acceso a repositorios.
   - Configuración de entornos de desarrollo segregados para pruebas y producción.
   - Copias de seguridad automáticas del código y bases de datos.
4. **Seguimiento y medición**

- Auditorías quincenales de commits en repositorios para detectar cambios no autorizados.
- Evaluaciones trimestrales de cumplimiento de las prácticas seguras por parte de los desarrolladores.

5. **Revisión y mejora**
   - Actualización de la política tras detectar un intento de phishing dirigido al equipo de soporte.
   - Inclusión de simulacros de respuesta ante incidentes como parte del entrenamiento anual.

3.6 Revisión

La revisión es un proceso planificado que garantiza que las políticas de seguridad sigan siendo pertinentes, eficaces y alienadas con los objetivos de la organización. Estas políticas tienen que evaluarse constantemente o cuando ocurran cambios que se consideran significativos, ya sea al interior o exterior de la empresa. Estos cambios se pueden dar por riesgos, amenazas, modificaciones legales o transformaciones de la organización.

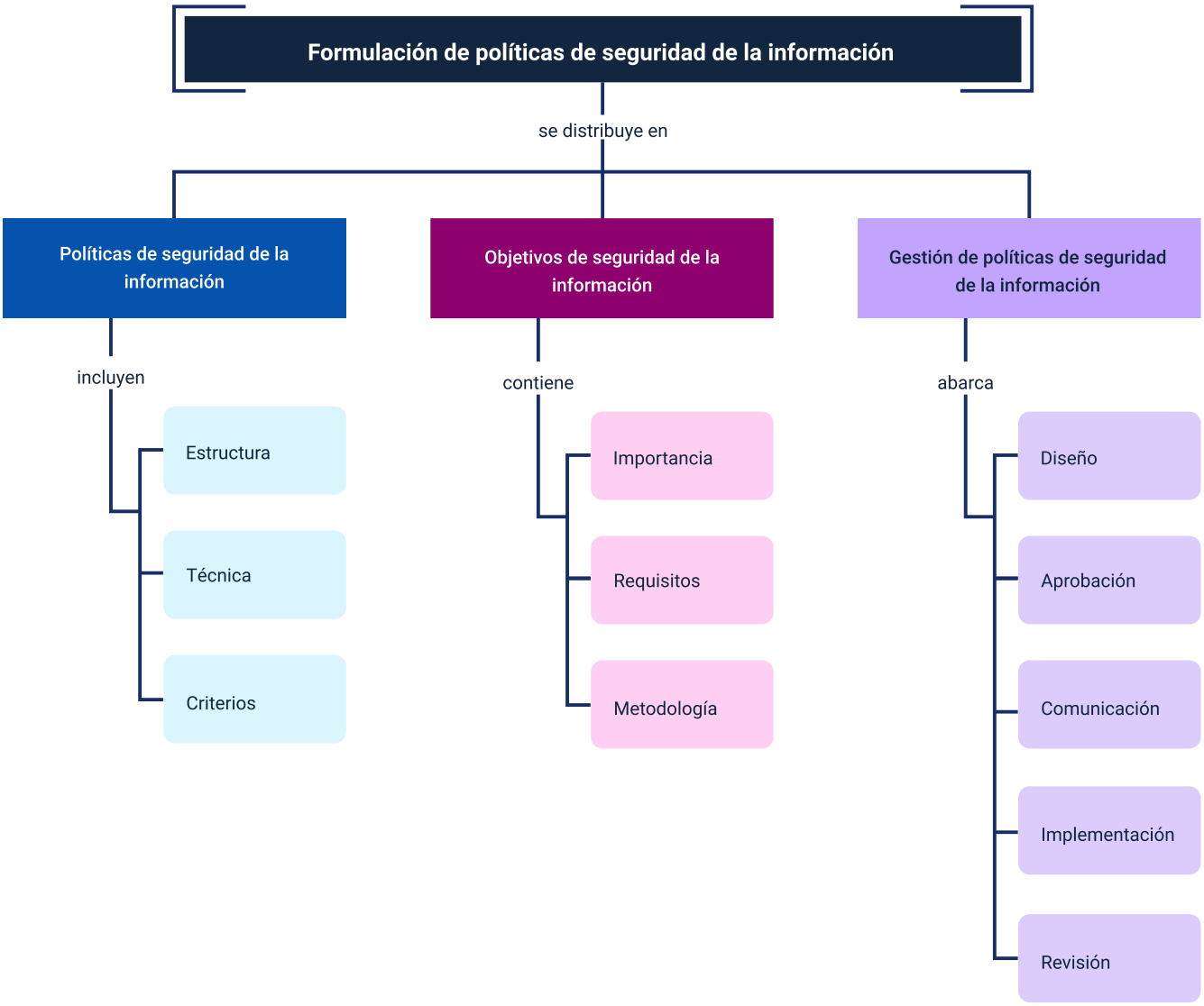
Aquí se analiza si las medidas y controles establecidos se están cumpliendo, si siguen respondiendo a los riesgos actuales o si es necesario reajustar en pro de la protección de los activos de información. La revisión tiene que ser documentada, contar con evidencias de seguimiento y si se consiguen errores, incumplimientos o desviaciones, definir planes de acción correctivos. En el caso de una pyme, según la consideración de su tamaño, pueden definir si la revisión la hace anual o semestral, involucrando a la dirección, a los responsables de áreas y al personal clave. Por ejemplo, la empresa agropecuaria El Buen Potrero, podría modificar su política después

de incorporar un nuevo software de monitoreo remoto para el ganado, mientras que la empresa PANAMSOFT, podría hacer la revisión, luego de implementar una nueva herramienta de desarrollo en la nube.

En cualquier caso, la revisión busca asegurar que las políticas evolucionen al mismo ritmo que los riesgos, la tecnología y las regulaciones, garantizando la mejora continua del sistema de gestión de seguridad de la información.

Síntesis

La formulación de políticas de seguridad de la información, sustentada en una estructura clara, técnicas de redacción adecuadas y criterios de alineación con las características de la organización, constituye la base para establecer directrices efectivas de protección. A su vez, la definición de objetivos de seguridad —claros, medibles y coherentes con las necesidades organizacionales— permite orientar las acciones hacia la preservación de la confidencialidad, integridad y disponibilidad de la información. La gestión de estas políticas, a través de etapas como su diseño, aprobación, comunicación, implementación y revisión, asegura su vigencia y efectividad, favoreciendo una cultura de cumplimiento normativo y de mejora continua dentro del Sistema de Gestión de Seguridad de la Información (SGSI).


Formulación de políticas de seguridad de la información
se distribuye en
Políticas de seguridad de la información
Objetivos de seguridad de la información
Gestión de políticas de seguridad de la información
incluyen
contiene
abarca
Estructura
Técnica
Criterios
Importancia
Requisitos
Metodología
Diseño
Aprobación
Comunicación
Implementación
Revisión

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Políticas de seguridad.	Cámara de Comercio de Honda. (s.f.). Política de seguridad.	Documento.	https://www.camarahonda.org.co/wp-content/uploads/2017/09/POLITICADESEGURIDADDELAINFORMACION.pdf
3. Gestión de políticas de seguridad de la información.	Acuña, G. (s.f.). Guía para escribir una política de Ciberseguridad en una empresa pequeña y Sitio web https://jaivatechnologies.com/guia-para-politica-de-ciberseguridad-en-pequena-mediana-empresa/mediana. Jaiva Technologies.	Sitio web.	https://jaivatechnologies.com/guia-para-politica-de-ciberseguridad-en-pequena-mediana-empresa/
3.5 Proceso de implementación.	LATAM Certificaciones TI. (2025, 10 de julio). CISO: Seguridad de la	Video.	https://www.youtube.com/watch?v=O3I8FXam9FE

Tema	Referencia	Tipo de material	Enlace del recurso
	Información: Plan de Implementación de Controles y Política de Seguridad de TI [Video]. YouTube.		

Glosario

Cultura organizacional: conjunto de valores, creencias y normas compartidas por los miembros de una organización, que influyen en su forma de trabajar y en la toma de decisiones. En seguridad de la información, determina el grado de compromiso de todos con la protección de los activos.

Gestión de políticas: proceso que abarca el diseño, aprobación, comunicación, implementación y revisión de políticas. En seguridad de la información, asegura que las políticas sean efectivas, actualizadas y alineadas con los objetivos de la organización.

Metodología: conjunto estructurado de pasos, técnicas y herramientas para desarrollar una tarea. En seguridad de la información, guía la formulación de políticas y la aplicación de medidas para proteger los datos.

Normativa: conjunto de leyes, estándares técnicos y buenas prácticas que orientan a las organizaciones en el diseño, implementación y cumplimiento de políticas de seguridad de la información.

Objetivo de seguridad: meta específica que busca proteger la confidencialidad, integridad y disponibilidad de la información. Debe ser clara, medible y alineada con las necesidades y requisitos legales de la organización.

Política de seguridad de la información: documento que establece las directrices y responsabilidades para proteger los activos de información. Sirve de base para políticas más específicas y para la gestión integral de la seguridad.

Pyme: organizaciones con recursos y personal limitados. En seguridad de la información, requieren políticas adaptadas a su tamaño y capacidades.

Seguridad de la información: disciplina que implementa medidas para proteger los datos de una organización, garantizando que se mantengan confidenciales, íntegros y disponibles ante cualquier tipo de amenaza.

Referencias bibliográficas

CYBERZONI. (s.f.). ISO27001 control 5.1 policies for information security.

https://cyberzoni.com/standards/iso-27001/control-5-1/

Duran, L. (2025, 11 de febrero). ¿Cómo se elabora la política general de seguridad? Docusign.com.

https://www.docusign.com/es-mx/blog/desarrolladores/politica-seguridad

Escuela Europea de Excelencia (EEE). (2022, 25 de octubre). Objetivos de seguridad de la información: guía de implementación para sistemas ISO 27001.

https://www.escuelaeuropeaexcelencia.com/2022/10/objetivos-de-seguridad-de-la-informacion-guia-de-implementacion-para-sistemas-iso-27001/

ESGinnova. (s.f.). 6.2. Objetivos de Seguridad de la información y planes para lograrlos.

https://www.pmg-ssi.com/norma-27001/6-2-objetivos-de-seguridad-de-la-informacion-y-planes-para-lograrlos/

Fortinet. (s.f.). ¿Qué es una política de seguridad de TI?

https://www.fortinet.com/lat/resources/cyberglossary/it-security-policy

Función Pública. (2020, marzo). Políticas de Operación Proceso de Tecnologías de la Información.

https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?

Morgan Hill. (s.f.). ISO/IEC 27002:2022.

https://www.morganhillcg.com/blog/item/iso-iec-27002-2022-5-1-policies-for-information-security-template

Orsys. (s.f.). Política de seguridad.

https://www.orsys.fr/orsys-lemag/es/glosario/politica-de-seguridad-%F0%9F%9F%A9-documento/

Parker, A. (s.f.). ISO 27001 control 5.1: Policies for information security. Iseo Blue.

https://iseoblue.com/post/iso-27001-control-5-1/

Piranirisk. (2022). Guía para hacer una Política de Seguridad de la Información.

https://www.piranirisk.com/es/academia/especiales/guia-politica-de-seguridad-de-la-informacion

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable Ecosistema de Recursos Educativos Digitales (RED)	Dirección General
Diana Rocio Possos Beltrán	Responsable de línea de producción	Centro de Comercio y Servicios - Regional Tolima
Armando Javier López Sierra	Experto temático	Centro de Comercio y Servicios - Regional Tolima
Andrés Felipe Velandia Espitia	Evaluador instruccional	Centro de Comercio y Servicios - Regional Tolima
Oscar Iván Uribe Ortiz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Lina Maria Pérez Manchego	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Diego Fernando Velasco Güiza	Desarrollador full stack	Centro de Comercio y Servicios - Regional Tolima
Sebastián Trujillo Afanador	Desarrollador full stack	Centro de Comercio y Servicios - Regional Tolima
Gilberto Junior Rodríguez Rodríguez	Animador y productor audiovisual	Centro de Comercio y Servicios - Regional Tolima
Norma Constanza Morales Cruz	Evaluadora de contenidos inclusivos y accesibles	Centro de Comercio y Servicios - Regional Tolima

Nombre	Cargo	Centro de Formación y Regional
Javier Mauricio Oviedo	Validador y vinculador de recursos educativos digitales	Centro de Comercio y Servicios - Regional Tolima