**ANEXO FORMATO COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Diseño de políticas en la gestión de la seguridad de la información |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501109. Diseñar modelo de seguridad de la información de acuerdo con estándares y marco de referencia. | RESULTADOS DE APRENDIZAJE | 220501109-01. Caracterizar las necesidades de seguridad de la información organizacional según riesgos, normativas y sistemas de gestión. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 01 |
| NOMBRE DEL COMPONENTE FORMATIVO | Fundamentos de un Sistema de Gestión de Seguridad de la Información |
| BREVE DESCRIPCIÓN | Este componente formativo aborda los fundamentos y herramientas para gestionar la seguridad de la información en entornos organizacionales, desde el reconocimiento de activos y valoración de riesgos hasta la formulación de políticas adaptadas. Incluye la estructura y normativa del Sistema de Gestión de Seguridad de la Información (SGSI), integrando principios de seguridad con un enfoque práctico, reflexivo y orientado a la aplicación real del conocimiento. |
| PALABRAS CLAVE | Activos, Gestión de riesgos, Normativa, Seguridad, SGSI. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | Ciencias naturales, aplicadas y relacionadas |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**

**Introducción**

**1. Activos de información**

1.1 Tipología

1.2 Registro

1.3 Valoración

**2. Seguridad de la información**

2.1 Concepto

2.2 Principios

**3. Gestión de riesgo**

3.1 Concepto

3.2 Tipos de riesgo

3.3 Fases

**4. Sistema de Gestión de Seguridad de la Información (SGSI)**

4.1 Concepto

4.2 Características y beneficios

4.3 Ciclo de mejora continua

4.4 Normativa

4.5 Componentes

1. **INTRODUCCIÓN**

En la actualidad las organizaciones tienen que funcionar no solo en el plano físico, sino en el digital, donde la información está considerada hoy en día, en uno de los activos más valiosos para ellas. Una adecuada gestión, protección y aprovechamiento de la información, representan desafíos que exigen competencias sólidas en seguridad, tanto a nivel físico, lógico y normativo. El uso intensivo de tecnologías de información y comunicación exponen a las empresas a un mayor número de amenazas digítales, lo que las obliga a que se necesite de un mayor grupo de profesionales que sean capaces de identificar activos críticos, vulnerabilidades, con el fin de aplicar principios de seguridad con criterio técnico y ético.

A través del estudio de activos, modelos de gestión de riesgo y los Sistemas de Gestión de Seguridad de la Información (SGSI), se desarrollan habilidades clave que lleven a las organizaciones a formular políticas y estrategias que respondan a las necesidades de protección de sus datos.

Por consiguiente, en este componente formativo, se busca ir más allá de la comprensión de conceptos fundamentales en seguridad de la información, para que los aprendices sean capaces de aplicar procesos en entornos reales. Además, se estimula una mirada crítica, reflexiva y contextualizada, alineada con una base sólida para la construcción de entornos digitales seguros, confiables, que estén en concordancia con estándares internacionales, para que se actúe con responsabilidad en el cambiante ecosistema informacional.

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

**DI\_ Guion\_Introduccion\_Video\_CF01\_21720209**

1. **DESARROLLO DE CONTENIDOS**

**1. Activos de información**

****

El punto de partida en un proceso de formación sobre gestión de la información, debe centrarse en los activos de información, ya que son ellos los que dan sentido a cualquier esfuerzo en materia de protección. No es posible implementar medidas de seguridad ni estructurar un sistema de gestión, si previamente no se ha definido qué se debe salvaguardar. Los activos representan el recurso esencial que se busca proteger y su identificación, clasificación y valoración, constituyen la base sobre la cual se toman decisiones estratégicas de seguridad. En este sentido, comenzar por los activos de información, permite establecer un enfoque claro y coherente, donde las acciones de protección no se aplican de forma genérica, sino con base en el valor real que cada activo representa para la organización.

A continuación, se presentan dos definiciones, la primera, teniendo de base el conocimiento y experiencia que pueden tener aquellas personas que ya entienden, conocen o han escuchado sobre seguridad de la información y la segunda, teniendo de base aquellas personas que no han escuchado del tema, pero que trabajan dentro de una organización:

|  |  |
| --- | --- |
| **Definición técnica** | Hablar de un activo de información, es referirse a cualquier recurso que tenga valor para la organización y que se encuentre directa o indirectamente en el ciclo de vida de la información (teniendo en cuenta la creación, el procesamiento, el almacenamiento, la transmisión y/o la destrucción si es el caso), para desarrollar el modelo de negocio. Aquí se incluyen elementos tangibles e intangibles, entre los que se pueden nombrar las bases de datos, los sistemas de información, libros contables, documentos físicos o digitales, procedimientos, manuales, personal, infraestructura y conocimiento organizacional, entre otros. |
| **Definición general** | Se puede llamar activo de información a todos aquellos recursos que usan las empresas para guardar, manejar o compartir información de interés para la organización. Hay que tener en cuenta, que la importancia no solo radica en los computadores o los archivos contenidos, aquí también entran los manuales del trabajo, las hojas de cálculo, los correos, las claves, incluso la experiencia y el conocimiento que tienen los empleados sobre su trabajo y todo aquello que tenga algún grado de información de la empresa y que permita su funcionamiento. |

Todos estos activos son importantes para que la empresa funcione correctamente, de ahí que se debe garantizar su seguridad; de lo contrario, si se presenta afectación en alguno de ellos, se podrían presentar pérdidas para la organización, que podrían ir desde obstruir un proceso, demorar un servicio, cancelar un negocio, hasta la liquidación misma de la actividad comercial.

Los activos de información son recursos que contienen datos valiosos para la organización y para la comunidad, por ello todas las empresas tienen que tenerlos identificados, actualizados y protegidos.

Los activos de información se clasifican en diferentes tipos según su naturaleza. Esta tipología facilita su identificación, protección y gestión adecuada dentro de las organizaciones.

* 1. **Tipología**

La clasificación de los activos de información, permite a las organizaciones saber qué deben proteger y cómo lo deben hacer; asimismo, la tipología facilita su identificación, protección y gestión adecuada dentro de la empresa. A continuación, se comparte la tipología según la Agencia Nacional Digital (AND) en Colombia, con una breve descripción y unos ejemplos para su mayor comprensión:

**Tabla 1.** *Tipología de activos de información (AND)*

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **Ejemplo** |
| **Información** | Datos estructurados o no estructurados que aportan valor a los procesos. | Bases de datos de clientes, reportes de ventas, historiales de compras, archivos Excel, documentos Word, formularios físicos o digitales. |
| **Tecnológicos o digitales** | Equipos y recursos tecnológicos que almacenan, procesan o transmiten información. | Computadores, celulares, *software* contable, sistemas POS, licencias de Office, discos duros externos, sistemas en la nube, páginas *web*, redes Wi-Fi. |
| **Infraestructura física** | Espacios e instalaciones necesarias para operar los sistemas de información. | Oficinas, *routers*, cableado de red, servidores físicos, cámaras de seguridad, sistemas de energía, puntos de acceso inalámbrico. |
| **Organizacional** | Conocimientos, procesos y estructuras organizativas que generan valor. | Procedimientos internos, instructivos, modelos de negocio, políticas de atención al cliente, servicios ofrecidos, metodologías de operación o ventas. |
| **Recurso humano** | Personas que conocen, generan o acceden a información crítica. | Vendedores, auxiliares contables, técnicos de soporte, contratistas, personal de logística, socios con conocimientos específicos del negocio, directores de departamentos. |

Elaboración propia con base en la Agencia Nacional Digital (AND) de Colombia

Tomando de base la norma ISO/IEC 27002, marco reconocido internacionalmente para gestionar la seguridad de la información, la cual permite a las pymes identificar, clasificar y proteger los activos de forma estructurada, facilitando el cumplimiento normativo y la reducción de riesgos operativos; se comparte otra tabla de ejemplo con la tipología referenciada en ella, con el fin de que se tenga otra referencia, aportando mayor claridad y comprensión al respecto:

**Tabla 2.** *Tipología de activos de información (ISO/IEC 27002)*

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **Ejemplo** |
| **Información** | Datos que tienen valor para la empresa, en formato físico o digital. | Facturas, contratos, listas de clientes, inventarios, bases de datos, hojas de cálculo, reportes financieros, correos electrónicos institucionales. |
| ***Software*** | Programas, aplicaciones o sistemas utilizados para gestionar información. | Sistemas contables (Siigo), CRM, aplicaciones de facturación, licencias de Windows, plataformas de ventas, *software* de diseño o gestión de inventario. |
| ***Hardware*** | Dispositivos físicos que procesan, almacenan o transmiten información. | Computadores, impresoras, celulares corporativos, servidores, memorias USB, cámaras de seguridad, *routers*, escáneres. |
| **Servicios** | Servicios que soportan procesos informáticos o de información. | Internet, servicios en la nube (Google Drive, Dropbox), *hosting web*, correo electrónico corporativo, soporte técnico, servicios de almacenamiento externo. |
| **Personas** | Individuos que interactúan con la información de la organización. | Gerente, auxiliar contable, encargado de bodega, administrador de sistemas, vendedores, mensajero, contratistas, practicantes. |
| **Conocimiento** | Saber técnico, experiencia y propiedad intelectual asociada al negocio. | Manuales internos, procedimientos, *know-how,* recetas, metodologías propias, procesos operativos documentados, instrucciones técnicas. |

Elaboración propia con base en la norma ISO/IEC 27002

Para clasificar los activos de información en una pyme, se recomienda aplicar una norma o estándar de base que permita seguir unas directrices, con el fin de facilitar la tarea y llevar una hoja de ruta que sirva de guía.

* 1. **Registro**

El registro de activos de información, es el proceso que se realiza dentro de la empresa u organización, para identificar, documentar y mantener actualizada toda la información relacionada con los activos que contienen, procesan o respaldan datos que son de interés para la actividad comercial. A parte de tener conocimiento de los activos que existen, con el registro también se busca saber dónde se encuentran, quién los utiliza, quién los administra y qué valor tienen esos activos para la pyme.

Con un buen registro de activos de información se puede:

* Tomar decisiones informadas en materia de seguridad.
* Asignar responsabilidades claras sobre cada uno de los activos de información.
* Evaluar y dar un tratamiento adecuado a los riesgos asociados a la información.
* Cumplir con la normatividad exigida, sobre todo, cuando se aplican estándares especializados, como por ejemplo la norma ISO/IEC 27001.
* Facilitar las auditorías y controles, especialmente cuando se cuenta con una fuente actualizada y confiable de los activos de información.

A continuación, se comparten los campos que se recomiendan para registrar los activos de información. Cabe destacar que muchas veces, estos campos pueden variar según las directrices de las empresas o la norma utilizada, pero por lo general tratan la misma información y son de gran ayuda para el inventario de activos:

* Código o identificación del activo.
* Tipo de activo.
* Descripción.
* Ubicación.
* Responsable del activo.
* Valor o criticidad.
* Clasificación de seguridad (confidencial, pública, restringida...).
* Estado de conservación o uso.

Con el siguiente ejemplo, se da una idea de cómo se podría llenar una tabla que contenga el registro de los activos de información de una pyme:

**Tabla 3***. Registro de activos de información clasificados por el campo valor/criticidad*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Código** | **Tipo de activo** | **Descripción** | **Ubicación** | **Responsable** | **Valor / Criticidad** | **Clasificación** | **Estado de conservación / Uso** |
| **AI-001** | Información | Base de datos de clientes con información personal y comercial. | Servidor local | Gerente de ventas | **Alta** | Confidencial | En uso / Actualizada |
| **AI-002** | Tecnológico / Digital | Computador del administrador con *software* contable y nómina. | Oficina principal | Administrador general | **Alta** | Confidencial | En uso / Buen estado |
| **AI-003** | Información | Registros contables y financieros electrónicos. | Sistema contable en la nube | Asistente contable | **Alta** | Confidencial | En uso / Accesible |
| **AI-004** | Recurso humano | Empleado con acceso privilegiado a datos sensibles. | Oficina administrativa | Jefe de talento humano | **Alta** | Confidencial | Activo / Funciones críticas |
| **AI-005** | Información | Contratos con proveedores y clientes. | Archivador físico y digital | Auxiliar administrativo | **Media** | Restringida | Conservados / Acceso controlado |
| **AI-006** | Tecnológico / Digital | Página *web* con formulario de contacto y base de datos simple. | *Hosting* externo | Coordinador de TI | **Media** | Pública | En uso / Actualizada |
| **AI-007** | Organizacional | Procedimientos internos de operaciones y logística. | Carpeta compartida | Director de operaciones | **Media** | Interna | Vigente / En revisión periódica |
| **AI-008** | Infraestructura física | Red Wi-Fi interna de uso empresarial. | Oficina principal | Coordinador de TI | **Media** | Restringida | Operativa / Estable |
| **AI-009** | Tecnológico / Digital | Impresora compartida conectada en red local. | Sala administrativa | Auxiliar administrativo | **Baja** | Interna | Operativa / Uso frecuente |
| **AI-010** | Información | Manuales de uso de equipos menores (cafetera, archivador). | Cocina / Tablero físico | Servicios generales | **Baja** | Pública | Vigente / Consultado ocasionalmente |

Teniendo en cuenta que el campo **Estado de conservación / Uso**, es uno de los que más puede causar confusión, en la siguiente tabla se amplía con descripciones y nuevos ejemplos, para que se puedan afianzar más los conocimientos y su aprendizaje:

**Tabla 4.** *Opciones para el campo “Estado de conservación / Uso”*

|  |  |  |
| --- | --- | --- |
| **Estado sugerido** | **Descripción** | **Ejemplo de aplicación** |
| **Activo / En uso** | El activo está operativo y siendo utilizado actualmente. | Computador de ventas, base de datos en producción. |
| **Activo / Consulta ocasional** | El activo se usa esporádicamente, pero sigue disponible. | Manual de procesos antiguos, informes históricos. |
| **Operativo / Requiere mantenimiento** | Funciona, pero requiere ajustes o revisión técnica. | *Router* con fallas intermitentes, impresora con atascos. |
| **Archivado / Conservado** | No se usa, pero se guarda por razones legales o administrativas. | Contratos de años anteriores, respaldos de contabilidad. |
| **Obsoleto / En desuso** | Ya no se utiliza, ni se considera útil, pero aún no ha sido eliminado formalmente. | *Software* incompatible, equipos sin soporte. |
| **En evaluación / En prueba** | Activo en fase de prueba o pendiente de implementación formal. | Nueva plataforma CRM en piloto, nuevo protocolo de seguridad. |
| **Dañado / Inservible** | No operativo; requiere reparación o eliminación. | Disco duro con daño físico, equipo con pantalla rota. |
| **Extraviado / No localizado** | El activo no ha sido encontrado en su ubicación habitual. | USB sin registro, documento físico perdido. |

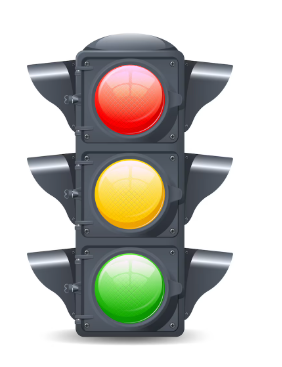
Como se percibe en los ejemplos anteriores, los campos del registro no necesitan llenarse exclusivamente con datos tomados de listas estandarizadas. Lo más importante es que cada pyme pueda comenzar a organizar su inventario de activos, según su realidad, construyendo un diccionario de datos propio que oriente la clasificación. En este proceso, es habitual que se nombren o clasifiquen activos por primera vez, lo cual contribuye al fortalecimiento de su gestión informacional.

Un claro ejemplo de esta flexibilidad se encuentra en el campo **Estado de conservación / Uso**, donde se han empleado diferentes expresiones como (En uso / Actualizado), (Operativo / Estable), (Archivado / Conservado) u (Obsoleto / En desuso). Aunque todas son válidas, su elección depende de cómo la empresa percibe y gestiona cada activo. Lo importante es mantener criterios claros y consistentes, aunque sean propios y que puedan evolucionar conforme madure el sistema de gestión de información.

**1.3 Valoración**

La valoración de los activos de información, es el proceso que puede utilizar una pyme para determinar el nivel de importancia o criticidad de cada uno de sus activos, logrando con ello establecer prioridades en su protección y administración. Esta valoración puede estipularse por el impacto que podría tener la pérdida, alteración o divulgación no autorizada de la información contenida en el activo, teniendo de base tres puntos fundamentales de la seguridad de la información:

Según la experiencia, naturaleza o actividad de la organización, cada una de ellas podrá definir las escalas de valoración, según su contexto; pero hay que tener en cuenta que una buena escala de valoración permitirá priorizar medidas de protección, basadas en el nivel de criticidad, ayudar a asignar recursos de seguridad en forma eficiente, además de contar con un insumo esencial para la gestión de riesgos. En ese orden de ideas, la clasificación de activos de información por su valoración, tomando de base normas como la **ISO/IEC 27005:2022, ISO/IEC 27001 e ISO/IEC 27002, se recomienda trabajarlas con las siguientes escalas de valoración:**



Baja

Media

Alta

* Alta

La pérdida, alteración o indisponibilidad del activo afectaría gravemente la operación o la reputación de la pyme.

Ejemplo: base de datos de clientes, información financiera, claves de acceso a plataformas.

* Media

Su afectación interrumpiría parcialmente procesos o generaría costos moderados.

Ejemplo: manuales de operación, correos internos, *software* de facturación.

* Baja

Su pérdida no compromete directamente la operación ni implica un riesgo significativo.

Ejemplo: publicidad impresa antigua, catálogos públicos, archivos duplicados no sensibles.

Tal como se ha podido analizar anteriormente, una buena valoración permite a las organizaciones identificar cuáles recursos requieren mayor protección, según su importancia para la actividad del negocio y la toma de decisiones. Este proceso ayuda en las acciones que hay que tomar en seguridad, la optimización de recursos y en las garantías que se dan para que los activos, principalmente los más críticos, puedan gestionarse de forma adecuada. De ahí, que, para las pymes, su implementación ayuda a fortalecer la confianza, la continuidad del negocio y mantener un mayor control sobre la información.

**2. Seguridad de la información**



Una vez identificados y valorados los activos de información, resulta necesario comprender los principios que orientan su protección dentro de las organizaciones. Es en este punto donde cobra sentido el estudio de la seguridad de la información. Esta disciplina no actúa de manera aislada, sino que se fundamenta en la importancia que cada activo representa para el cumplimiento de los objetivos institucionales, permitiendo establecer niveles adecuados de protección frente a amenazas internas y externas que puedan sufrir las pymes.

**2.1 Concepto**

Es fundamental entender qué es la seguridad de la información y el por qué, se hace necesario establecer mecanismos de protección en cualquier empresa; por ello, a continuación, se presentan dos definiciones, ajustadas a diferentes niveles de comprensión y contexto:

|  |  |
| --- | --- |
| **Definición técnica** | La seguridad de la información, también conocida como InfoSec, comprende el conjunto de estrategias, normas y mecanismos orientados a garantizar que la información, sin importar su forma o medio, se mantenga confidencial, íntegra y disponible. Su finalidad es prevenir accesos no autorizados, modificaciones no deseadas o pérdidas, asegurando que los datos sean gestionados de forma segura y confiable en el desarrollo de las actividades organizacionales (IBM, 2024a).  La seguridad de la información, hace referencia al conjunto de prácticas, herramientas y procedimientos orientados a proteger la información confidencial de una organización frente a accesos no autorizados, usos indebidos, interrupciones o destrucción. Este enfoque abarca tanto la seguridad física y del entorno, como los mecanismos de control de acceso y las medidas de ciberseguridad, integrando una visión integra de protección de la información (Microsoft, s.f.). |
| **Definición general** | La seguridad de la información es el conjunto de medidas que se aplican para cuidar toda la información de la empresa. Cuando se habla de cuidarla, se hace referencia a que personas que no estén autorizadas no pueden tener acceso a ella o evitar que sea modificada por error o por mal uso, también garantizar que esté disponible cuando las personas autorizadas la necesiten.  Para entender mejor, así como la bodega donde se guarda la mercancía que vende un almacén está protegida con llaves e incluso cámaras de videos, asimismo, la información debe protegerse, sin importar que esté en papeles, computadores u otros dispositivos informáticos y que el acceso a ella solo lo tendrán aquellas personas que han sido previamente autorizadas para su visualización, revisión, o hasta modificación. |

Lograr comprender el papel que juega la seguridad de la información, permite a las pymes, proteger sus activos más valiosos, frente a riesgos que puedan comprometer su funcionamiento. Este trabajo integral garantiza que la información se mantenga confiable, accesible y libre de alteraciones; por lo que hay que tener claro que la seguridad de la información no solo debe ser vista como una medida técnica, sino más bien como una responsabilidad estratégica en todos los niveles de la organización.

Luego de entender qué es la seguridad de la información y su propósito en las pymes, se invita a conocer los principios que la sustentan, ya que así se puede orientar a una aplicación más práctica y tomar decisiones más acertadas en la protección de los activos de información.

**2.2 Principios**

Toda gestión de la información en una empresa debe fundamentarse en tres principios esenciales (la confidencialidad, la integridad y la disponibilidad de la información), para poder cumplir con los criterios de eficiencia y eficacia, y así garantizar un sistema seguro y confiable (Novasep, s.f.). Estos principios constituyen la base sobre la cual se diseñan las políticas, controles y procedimientos para proteger los activos de información en una organización.

También hay se debe tener en cuenta que estos principios, no solo guían la implementación técnica de medidas de seguridad, sino que también ayudan en la toma de decisiones alineadas con los objetivos estratégicos y la normativa de la empresa.

Comprender estos tres pilares, es clave para establecer medidas efectivas, así que a continuación, se describen y se sustentan con ejemplos cada uno de ellos:

* **Confidencialidad**

Consiste en garantizar que la información solo sea accesible por personas autorizadas. Se refiere a la protección frente al acceso no autorizado, ya sea accidental o intencional. Aplicar este principio implica establecer políticas de control de acceso, gestión de credenciales y protección frente a fugas de información.

Ejemplos prácticos en pymes:

* Uso de contraseñas seguras para acceso a sistemas.
* Restringir el acceso a datos contables solo al área financiera.
* Implementar roles diferenciados en *software* de gestión.
* **Integridad**

Asegura que la información se mantenga completa, precisa y sin alteraciones no autorizadas. La integridad implica que los datos no sean modificados, eliminados o creados de forma inapropiada, ya sea por error o por intervención maliciosa.

Ejemplos prácticos en pymes:

* + - Copias de respaldo que permiten recuperar versiones anteriores de documentos.
    - Registro de auditoría que evidencia cambios realizados en los sistemas.
    - Validación de formatos o formularios antes de ingresarlos en una base de datos.
* **Disponibilidad**

Se refiere a que la información esté disponible y accesible cuando se requiera por los usuarios autorizados. Este principio implica garantizar el funcionamiento continuo de los sistemas y el acceso oportuno a los recursos informáticos necesarios para la operación del negocio.

Ejemplos prácticos en pymes:

* + - Sistemas de respaldo energético (UPS) para evitar pérdida de datos en apagones.
    - Políticas de mantenimiento preventivo para evitar fallas en equipos.
    - Copias de seguridad periódicas y accesibles en caso de incidentes.

Estos principios tienen que reflejarse en las políticas de seguridad de la información, asegurando que cada uno esté presente en los lineamientos generales y específicos. Por ejemplo, en una pyme, una política de contraseña contribuye a la confidencialidad, una política de respaldo fortalece la disponibilidad y una política de control de cambios protege la integridad de la información.

**3. Gestión de riesgo**



La gestión de riesgos en seguridad de la información, es el proceso que identifica, analiza y controla las amenazas que pueden afectar a los activos de información; por ende, entender este proceso, permite que se puedan gestionar decisiones estratégicas que fortalezcan la protección de la información y garanticen la continuidad del negocio. Para mayor comprensión, se abordarán aspectos claves que permitan estructurar una gestión efectiva del riesgo, tocando desde un concepto más profundo, hasta las fases que conforman un tratamiento sistemático.

**3.1 Concepto**

Para comprender mejor que significa gestionar riesgos en seguridad de la información, se proporcionarán unas definiciones desde el punto técnico y desde una visión general y se apoyarán dichos conceptos con ejemplos de la vida cotidiana, realidades que son comunes en las pymes colombianas, de tal manera que se dimensione el porqué de su importancia y se justifique su aplicación:

|  |  |
| --- | --- |
| **Definición técnica** | Consiste en identificar, priorizar, controlar y supervisar las amenazas que pueden afectar los sistemas de información y los activos digitales de una organización (IBM, 2024b).  La gestión de riesgos en ciberseguridad es un proceso enfocado en identificar, analizar, medir y controlar los riesgos que afectan la seguridad de la información. Su propósito es anticiparse a las amenazas mediante la implementación de controles preventivos que reduzcan su impacto. Esta gestión se aplica en diversos ámbitos de la organización y requiere que los responsables reconozcan los riesgos que pueden afectar sus objetivos. De hecho, más del 70 % de las empresas ha experimentado problemas relacionados con la ciberseguridad, sin importar su tamaño o sector (Grupo Cibernos, s.f.). |
| **Definición general** | La gestión de riesgos en seguridad de la información consiste en identificar los peligros que pueden afectar la información de una empresa, tales como los ataques por internet, los errores humanos o la pérdida de datos, entre otros. Esta gestión sirve para que se puedan tomar decisiones y aplicar medidas que ayuden a prevenir esos problemas antes de que ocurran, protegiendo así la información del negocio y evitando pérdidas o interrupciones. |

Para comprender mejor cómo se aplica la gestión de riesgos en la seguridad de la información, es útil revisar unos ejemplos desde la realidad de las pymes colombianas; estas situaciones permiten visualizar los riesgos comunes y formas en que pueden prevenirse o disminuirse con acciones sencillas pero efectivas:

|  |
| --- |
| **Taller de confecciones Gala** |
| En el taller de confecciones Gala, en el centro de Medellín, los pedidos, las fechas de entrega, las cantidades y los datos de contacto de los clientes, se registran en un computador portátil. Un día por accidente, el computador se extravía y la empresa no puede cumplir con varios encargos, lo que genera incumplimiento a la empresa, pérdidas económicas y mala imagen ante los clientes que esperaban el pedido.  Esta situación evidencia un riesgo claro, ya que la pérdida de información es crítica, por no contar con los respaldos. Una gestión de riesgos adecuada habría permitido identificar este peligro y tomar medidas preventivas, como almacenar copia de la información en Google Drive o en un disco externo. |
| **Papelería Maicao** |
| La papelería Maicao, ubicada en Fontibón, guarda la información de su inventario, proveedores y cuentas por pagar en el computador de escritorio que maneja la administradora de la papelería, el cual no cuenta con antivirus, mucho menos actualizaciones recientes de su sistema operativo. El hijo de la administradora, que pasó la mañana en la papelería, ya que no pudo ir a clases porque ese día la habían suspendido, decidió descargar Roblox para no pasarse el rato aburrido. Estuvo jugando con otros usuarios durante dos horas, tiempo en el que interactuaron vía *chat* e intercambiaron algunos archivos para aprovechar algunos recursos del juego. De repente el sistema se bloqueó y lo archivos quedaron inutilizables por un *ransomware*.  Este incidente pudo haberse prevenido si se hubiera aplicado una gestión de riesgos básica que incluyera medidas como el uso de *software* de protección, copia de seguridad de los datos, así como políticas de restricción de uso de equipos para labores de la papelería por personal autorizado. |
| **Finca de cría y venta de cabras en la Guajira** |
| En la finca La Costa, ubicada en la Guajira, se realiza el seguimiento del crecimiento, alimentación y vacunación de los animales en una libreta física. Un día, un fuerte aguacero que se inicia de repente, moja parte de la libreta que se encontraba recostada a una de las madrinas del corral, dañando algunos registros. Por el aguacero, tuvieron que suspender la vacunación y desparasitación de los animales. Dos semanas después retomaron el proceso, pero cómo parte de las hojas que contenían esa información habían sido dañadas por el agua, les tocó realizar el procedimiento nuevamente a todos los animales, incluyendo los que habían vacunado y desparasitado en la jornada anterior.  Con una adecuada gestión de riesgos, se habrían tomado correctivos, entendiendo que el uso de registros físicos sin copia era un punto vulnerable. Como acción, se podrían tener digitalizado los datos en una aplicación sencilla o en Excel, respaldadas en el celular o en la nube. Esto garantizaría la continuidad del negocio, aún frente a incidentes climáticos o imprevistos. |

Comprender qué es la gestión de riesgos en seguridad de la información, permite a las pymes anticiparse a las amenazas que puedan afectar sus procesos y activos de información. Identificar y analizar los riesgos no solo ayuda a prevenir pérdidas, sino que fortalece la toma de decisiones y promueve una cultura organizacional más segura y preparada ante posibles incidentes.

**3.2 Tipos de riesgo**

Al buscar en diferentes fuentes, es fácil deducir que hay múltiples formas de clasificar los riesgos de seguridad de la información, esto se da por la diversidad de enfoques y contextos organizacionales. Lo variado de estas clasificaciones es porque los riesgos pueden provenir de ámbitos técnicos, humanos, físicos, procedimentales o de terceros, según el objetivo o la experiencia de cada modelo de gestión. Esta multiplicidad de perspectivas se confirma en estudios académicos que revisan y comparan las diferentes taxonomías de riesgos en entornos de seguridad de la información (Rabitti et al., 2025).

Por lo anterior, se relaciona una clasificación detallada de los tipos de riesgos en seguridad de la información, donde se presenta una visión amplia y actualizada de las principales amenazas, tales como ciberataques, brechas de seguridad, fallos tecnológicos o riesgos de cumplimiento, que reflejan la diversidad de escenarios que enfrentan las organizaciones en la práctica y cuya perspectiva aplicada facilita la identificación y el manejo de riesgos en entornos reales (GRCTools, s.f.):

|  |  |
| --- | --- |
|  | **Descripción** |
|  | **Ciberseguridad**  Amenazas digitales que pueden comprometer los sistemas o la confidencialidad de los datos.  **Riesgo:**  *Malware, phishing*, ataques DDoS, ingeniería social, filtración de información. |
|  | **Infraestructura tecnológica**  Riesgos derivados de fallos físicos, tecnológicos o eventos naturales que afectan los sistemas o la operación tecnológica.  **Riesgo:**  Caídas de servidores, errores de *software*, incendios, terremotos. |
|  | **Acceso y autenticación**  Vulnerabilidades relacionadas con el ingreso indebido a sistemas o la debilidad en los mecanismos de verificación.  **Riesgo:**  Contraseñas débiles, accesos sin permisos, ausencia de autenticación multifactor. |
|  | **Cumplimiento y regulaciones**  Incumplimiento de normativas legales o falta de políticas internas que regulen la seguridad de la información.  **Riesgo:**  Falta de cumplimiento de GDPR, HIPAA; ausencia de procedimientos documentados. |
|  | **Riesgos humanos**  Comportamientos, errores o negligencias del personal que exponen los sistemas o los datos a amenazas.  **Riesgo:**  Errores accidentales, empleados que actúan con intención de dañar. |
|  | **Terceros**  Amenazas que provienen de empresas o individuos externos que acceden o manejan información de la organización.  **Riesgo:**  Fallas de proveedores, subcontratistas con manejo de datos sensibles. |

Para mayor comprensión de los tipos de riesgos compartidos previamente, se exponen ejemplos situacionales dentro de una pyme que permiten entender mejor cada uno de ellos:

* **Ciberseguridad**

Una tienda virtual de productos artesanales es víctima de un ataque de *ransomware* que cifra toda su base de datos de clientes, pedidos e inventario. Los ciberdelincuentes solicitan un rescate en criptomonedas para liberar la información. La empresa no contaba con copias de seguridad actualizadas y se ve obligada a suspender sus operaciones por varios días, perdiendo ventas y afectando su reputación.

* **Infraestructura tecnológica**

Un taller industrial sufre un daño eléctrico por un cortocircuito, lo cual afecta el servidor donde almacena cotizaciones, facturación y archivos técnicos de los equipos. La ausencia de un sistema de respaldo de energía y una copia de seguridad externa genera la pérdida total de información crítica para la operación del negocio.

* **Acceso y autenticación**

En un taller de diseño gráfico, varios colaboradores comparten la misma contraseña para acceder al servidor donde guardan los proyectos de clientes. Un exempleado, al que no se le revocaron los permisos, accede de forma remota y elimina varios archivos, causando retrasos en entregas importantes y pérdidas económicas.

* **Cumplimiento y regulaciones**

La clínica Perritos recolecta datos personales de sus clientes, sin contar con un aviso de privacidad ni mecanismos claros de protección de la información. Durante una inspección, es sancionada por la Superintendencia de Industria y Comercio, por incumplir la Ley 1581 de 2012 sobre protección de datos personales, enfrentando una multa y la obligación de implementar controles en poco tiempo.

* **Riesgos humanos**

En Cauchos El Estirón, un trabajador sin formación en gestión documental, elimina sin querer, una carpeta compartida en la nube, que contenía planos y diseños de un nuevo cliente. Esta pérdida obliga a repetir el trabajo desde cero, afectando la entrega y la confianza del cliente.

* **Terceros**

La distribuidora Frescos Bosconia, contrata a un proveedor externo para desarrollar una aplicación móvil de pedidos. El proveedor deja una vulnerabilidad abierta en el sistema, la cual es aprovechada por atacantes para robar información de clientes y suplantar pedidos. La empresa, al no haber firmado un contrato con cláusulas claras de seguridad, enfrenta la situación sola.

Identificar y comprender los diferentes tipos de riesgos en seguridad de la información, son pasos esenciales para las operaciones diarias, en las diferentes empresas y organizaciones. Teniendo en cuenta que la mayoría de empresas pequeñas como las pymes, carecen de infraestructura tecnológica robusta o de personal especializado, es de mucha ayuda conocer las amenazas más comunes, con el fin de que estén alertas y puedan ir tomando decisiones informadas, según las situaciones que se vayan presentando; asimismo, poder ir implementando medidas básicas de protección y previniendo pérdidas que puedan afectar gravemente la sostenibilidad y continuidad de las empresas. De ahí la importancia de que las directivas se sintonicen con una conciencia y acción temprana, para fortalecer la competitividad, frente a los clientes, aliados y entornos digitales cada vez más exigentes.

**3.3 Fases**

La gestión de riesgos en seguridad de la información, según la norma ISO/IEC 27005, se desarrolla mediante un enfoque sistemático dividido en seis fases, cada una con un papel clave para proteger los activos. Dentro de la fase de evaluación del riesgo se integran tres subprocesos esenciales, que en algunos enfoques pueden presentarse como etapas independientes, lo que explica posibles variaciones al consultar otras fuentes. Este proceso no se limita a identificar amenazas, sino que busca actuar de forma preventiva y estratégica. Se aclara para que no se pierda la coherencia del enfoque normativo, al investigar otras fuentes.

Por lo anterior, a continuación, se detallan estas fases con su descripción, para facilitar su comprensión y aplicación en contextos empresariales, según la norma ISO/IEC 27005, a partir de It Governance (2022):

|  |  |
| --- | --- |
| **1. Establecimiento del contexto** | El contexto de la gestión de riesgos define las pautas para identificar los riesgos, asignar responsabilidades sobre su gestión, analizar su impacto en la confidencialidad, integridad y disponibilidad de la información, así como determinar cómo se evalúan la probabilidad y las consecuencias de su ocurrencia. |
| **2. Evaluación del riesgo** | Comprende tres subprocesos interrelacionados:   * **Identificación:** reconoce las amenazas, las vulnerabilidades y los activos que están expuestos a los posibles incidentes de seguridad. * **Análisis:** se estima la probabilidad y el impacto de los riesgos, además de hacer consideración de los controles existentes. * **Valoración:** se estiman y comparan los niveles de riesgo con criterios definidos, con el fin de decidir si hay necesidad de aplicar un tratamiento. |
| **3. Tratamiento del riesgo** | Después de la valoración de los riesgos, se decide cómo abordarlos: tratando inicialmente de evitarlos al eliminar la causa por completo, modificándolos al aplicar los controles disponibles, transfiriendo el riesgo a un tercero por medio de un seguro o un contrato o aceptándolos si estos se encuentran dentro de un umbral de tolerancia al cumplir con unos criterios de aceptación. |
| **4. Aceptación del riesgo** | Aquí se documentan aquellos riesgos que tras un tratamiento no pudieron ser eliminados, pero la empresa decide aceptarlos porque pueden ser tolerables; para ello, tiene que justificarlos con base en un análisis costo-beneficio, viabilidad técnica o estratégica. |
| **5. Comunicación y consulta** | Es importante asegurar que todos los interesados en la organización estén informados sobre los riesgos, con la finalidad de que las decisiones y acciones a tomar sean entendidas y adoptadas por todos. |
| **6. Monitoreo y revisión** | Los riesgos tienen que estar monitoreados constantemente, ya que pueden tener cambios de forma intempestiva, así que siempre se tiene que estar revisando para tener como actuar enseguida y no encontrarse con sorpresas que puedan hacer a un lado todo el trabajo de la empresa. |

Aplicar estas fases de la gestión de riesgos, fortalece en las diferentes empresas u organizaciones sus capacidades para anticiparse y responder efectivamente ante posibles amenazas que puedan afectar la información. Es una manera de enfocarlas para que se mantengan en prevención y en mejora continua; además de proteger los activos críticos y de alinear la seguridad con los objetivos estratégicos, especialmente en un mundo en donde los procesos en su mayoría se están manejando de forma digital y donde se viven adoptando diferentes tecnologías, que hacen que los procesos sean cambiantes.

**4. Sistema de Gestión de Seguridad de la Información (SGSI)**

****

Después de la identificación y valoración de los activos de información y del análisis de los riesgos, es necesario contar con un buen sistema que permita aplicar y gestionar la protección de manera continua; para ello, un Sistema de Gestión de Seguridad de la Información (SGSI), proporciona un marco integral, que contiene las políticas, los procesos y los controles, con los cuales se pueda garantizar en la organización la confidencialidad, la integridad y la disponibilidad de la información.

**4.1 Concepto**

Entender qué es un Sistema de Gestión de Seguridad de la Información (SGSI), es de suma importancia para la protección de los datos de la organización; por ello, a continuación y para seguir la linealidad temática de los diferentes conceptos tratados, se comparten dos definiciones, una técnica desde la visión de una fuente oficial y otra en un lenguaje más sencillo, con la finalidad de que sea más digerible para aquellos incursionan en este mundo por primera vez:

|  |  |
| --- | --- |
| **Definición técnica** | Se concibe como una estructura organizada y conformada por políticas, procedimientos, directrices, recursos y tareas gestionadas en forma conjunta y articulada por una organización para la protección de sus activos de información. De acuerdo con la norma ISO/IEC 27001, este sistema adopta un enfoque metodológico que permite establecer, implementar, supervisar, evaluar, mantener y perfeccionar la seguridad de la información, asegurando su alineación con sus objetivos estratégicos (López, 2013). |
| **Definición general** | Es una forma organizada de cuidar y proteger la información importante de una empresa, como datos de clientes, documentos de trabajo o claves de acceso. Todo esto ayuda a evitar que la información se pierda, se dañe o caiga en manos no autorizadas. También establece reglas y buenas prácticas para que todos los empleados de una organización sepan cómo actuar y proteger la información que manejan a diario. |

Comprendido el concepto, no se puede desconocer que la implementación de un SGSI, es importante para garantizar la protección de la información más relevante, dentro de la organización, lo que ayuda a gestionar los riesgos de forma estructurada y alineada con los objetivos institucionales; además de brindar confianza dentro y fuera de la organización.

**4.2 Características y beneficios**

El comprender las características y beneficios de un SGSI, permite valorar la importancia que esta reviste al interior de una organización, especialmente cuando estas buscan proteger sus activos de información; por ende, una implementación no solo garantiza su seguridad, sino que le aporta valor agregado a la misma.

A continuación, se explica más en detalle el beneficio que presenta cada característica:

1. **Enfoque basado en riesgos**

Ayuda a que se identifiquen, evalúen y se prioricen los riesgos que afectan a los activos de información de la empresa.

1. **Mejora continua**

Es el proceso que favorece la revisión constante del sistema, de tal manera que se fortalezca su eficacia, frente a las diversas amenazas, principalmente frente a las nuevas o a las que son cambiantes.

1. **Marco normativo estructurado**

Con esto se asegura el cumplimiento de estándares nacionales e internacionales y de las buenas prácticas en seguridad de la información.

1. **Participación de todos los niveles de la organización**

Es importante y a la vez recomendable para que se puede fomentar una cultura organizacional de seguridad y corresponsabilidad, entre todos los actores; de lo contrario, no tendría gracia la implementación del SGSI, si lo planteado no se va a aplicar.

1. **Documentación y trazabilidad de procesos**

Esto facilita que se puedan realizar auditorías, también mejora la toma de decisiones y minimiza los errores por falta de control.

1. **Adaptabilidad al tamaño y sector de la empresa**

Lo importante de esto es que pueden ajustar diferentes organizaciones y empresas, sin importar su tamaño.

1. **Soporte para la toma de decisiones estratégicas**

Proporciona información clara sobre los riesgos y controles, que permiten alinear la seguridad con los objetivos y la actividad del negocio.

1. **Reducción de incidentes de seguridad**

Se busca eliminar o minimizar las pérdidas económicas y de reputación por accesos no autorizados, filtraciones o errores humanos, entre otros.

Conocer las características y beneficios del SGSI, permite entender el papel que este sistema representa en la protección de la información y cómo su implementación fortalece la seguridad de la información, mejora los procesos y aporta confianza a todos sus clientes y sus aliados.

**4.3 Ciclo de mejora continua**

Parte del éxito de la implementación de un SGSI, es el ciclo de mejora continua, ya que es el que permite que se mantenga y se perfeccione de forma progresiva, sosteniéndose en el tiempo. Este proceso se estructura por lo general bajo el modelo PHVA (Planificar, Hacer, Verificar y Actuar), también conocido como el ciclo Deming o PDCA (por sus siglas en inglés).

El ciclo de mejora continua en un SGSI, busca alinearse con un marco normativo, para garantizar que las políticas, controles y procesos del sistema, se mantengan ajustadas a los riesgos emergentes, a los cambios de la empresa y al entorno tecnológico, que es el que hoy en día más cambio sufre dentro de la organización.

A continuación, se explica cada uno de los pasos que lleva un ciclo de mejora continua bajo el modelo PHVA:

1. **Planificar (*Plan*)**

Se definen los objetivos del SGSI, las políticas y los procesos para que se puedan gestionar los riesgos que se han identificado. Aquí mismo, se establecen los criterios de evaluación y los recursos que se requieren para ello.

1. **Hacer (*Do*)**

Se implementan las políticas y los controles que se han definido, desarrollando las acciones que planificaron y aplicando las medidas de seguridad que se habían acordado.

1. **Verificar (*Check*)**

Se le hace seguimiento al SGSI y se evalúa su desempeño, analizando cada uno de los resultados obtenidos, frente a los objetivos que se habían establecido. Dentro de este punto están las auditorías internas, la revisión de los indicadores y el análisis de los incidentes.

1. **Actuar (*Act*)**

De acuerdo a los resultados obtenidos, se van adoptando medidas correctivas o de mejora, ajustando los procesos, las políticas y los controles, de tal manera, que se vaya fortaleciendo en sistema dentro de la organización.

Este ciclo de mejora continua, es importante porque fomenta una cultura organizacional, orientada al aprendizaje y a la adaptación continua, con lo que se logra responder de manera oportuna y eficiente a nuevas amenazas y vulnerabilidades, lo que conlleva que el SGSI implementado se mantenga vigente y en constante evolución junto a los desafíos del entorno digital.

**4.4 Normativa**

La normativa en seguridad de la información, proporciona los lineamientos que se necesitan para establecer, operar, mantener y operar un SGSI de manera efectiva. Estas normas permiten a las organizaciones adoptar prácticas que son aceptadas nacional o internacionalmente, gestionar sus riesgos y cumplir con exigencias legales, contractuales o sectoriales. Cabe aclarar, que muchas veces, aplicar estas normativas, exige a las empresas un esfuerzo económico y logístico.

A continuación, se presenta un conjunto de normas que pueden aplicarse, según la naturaleza y actividad de la empresa, iniciando con las que tienen jurisdicción a nivel internacional:

1. **ISO/IEC 27001**

Es una norma internacional que establece requisitos para la implementación y sostenimiento de un SGSI, aportando una base y promoviendo un enfoque por procesos y mejora continua.

1. **ISO/IEC 27002**

Complementa la norma ISO/IEC 27001, ofreciendo un conjunto de controles de seguridad, los cuales pueden irse adoptando según el contexto y tamaño de la empresa.

1. **ISO/IEC 27005**

Proporciona directrices para la gestión de riesgos de seguridad de la información, siendo crucial en la toma de decisiones basadas en análisis y evaluación de riesgos.

1. **ISO/IEC 27701**

Norma centrada en la gestión de la privacidad de la información (extensión de la ISO 27001), ideal para organizaciones que procesan datos personales.

1. **NIST SP 800-53**

Publicación del NIST que establece controles de seguridad y privacidad para sistemas de información federales y empresariales.

1. **GDPR (UE)**

Reglamento General de Protección de Datos europeo que regula el tratamiento de datos personales y la privacidad.

1. **MAGERIT**

Metodología española para el análisis y gestión de riesgos en sistemas de información, ampliamente usada en instituciones públicas.

1. **COBIT**

Marco de gobierno y gestión de TI que incluye prácticas de control de seguridad, alineadas con los objetivos del negocio.

1. **ITIL**

Biblioteca de buenas prácticas para la gestión de servicios de TI, incluyendo la gestión de incidentes y seguridad de la información.

Ahora, se detallan las que tienen jurisdicción nacional solo en Colombia:

* **Ley 1581 de 2012**

Regula la protección de datos personales en Colombia y exige a las organizaciones implementar medidas que garanticen el tratamiento adecuado de la información.

* **Decreto 1377 de 2013**

Complementa la Ley 1581 de 2012, estableciendo condiciones para la autorización del tratamiento de datos y medidas administrativas en entornos digitales.

* **Ley 1266 de 2008**

Ley de Habeas Data financiera. Regula el uso de la información financiera, crediticia, comercial y de servicios.

* **Ley 1273 de 2009**

Introduce delitos informáticos en el código penal colombiano, protegiendo la confidencialidad, integridad y disponibilidad de la información.

* **Circular Externa 005 de 2017 (SIC)**

Orienta a los responsables del tratamiento de datos sobre el cumplimiento de las leyes de protección de datos.

* **CONPES 3701 de 2011**

Política pública que impulsa el uso de estándares de gestión del riesgo, continuidad de negocio y seguridad de TI en el Estado colombiano.

Estas normas, marcos o leyes guían y dan las directrices a las empresas para que puedan proteger sus activos de información más preciados y garantizar la confianza de clientes, empleados, aliados y todas las partes interesadas. Su adopción es útil para las pymes, sobre todo porque al estar en un proceso de crecimiento, es primordial garantizar la seguridad de la información, para que la empresa pueda mantenerse en el tiempo.

**4.5 Componentes**

Para poner a funcionar un SGSI de manera que trabaje efectiva y eficazmente, es necesario que se comprendan ciertos componentes que son claves y que se hacen esenciales para la construcción de una estructura sólida, que permita salvaguardar de forma adecuada la información en el entorno organizacional. A continuación, se presentan los principales componentes, de acuerdo a lo expuesto por Kantan (2024):

* **Políticas de seguridad de la información**

Establece las directrices generales que utiliza la organización para demostrar su compromiso con la protección de la información. Estas políticas sirven para orientar las acciones, definir las responsabilidades y reflejar los objetivos que guíen la implementación del SGSI en los diferentes niveles.

* **Evaluación de riesgos**

Es el proceso sistemático para la identificación y el análisis de las amenazas potenciales en las que podría verse envuelta la seguridad de los activos de información de una empresa. Permite desarrollar la estimación de la probabilidad y el impacto de los riesgos, facilitando su clasificación y priorización, según su criticidad, lo cual es de suma importancia para tomar decisiones informadas.

* **Control y mitigación de riesgos**

Después de que sean identificados y evaluados los riesgos, hay que establecer e implementar medidas con la finalidad de disminuir su impacto o su probabilidad de ocurrencia. Dentro de estas acciones se pueden incluir herramientas tecnológicas, controles físicos y digitales, prácticas organizativas, diseñadas y ajustadas para salvaguardar la información sensible.

* **Monitorización y revisión**

Esto implica el seguimiento y monitoreo constante del funcionamiento del SGSI, con el propósito de garantizar que los controles aplicados sean eficaces y pertinentes. Todo esto se logra gracias a la ejecución de auditorías internas, a la revisión de indicadores que se consideren clave en el proceso y al análisis de los incidentes, con el fin de ir promoviendo y realizando ajustes y mejoras continuas.

La aplicación efectiva de los componentes que se consideran clave en un SGSI, ayuda para que las organizaciones construyan una estructura sólida para que puedan proteger con mayor confianza sus activos de información. Cada uno de componentes contribuye de forma integrada en garantizar los principios básicos como lo son la confidencialidad, la integridad y la disponibilidad de los datos.

1. **SÍNTESIS**

La adecuada identificación, registro y valoración de los activos de información, permite reconocer su importancia estratégica y asignar medidas de protección acordes a su valor y criticidad. Esta gestión, fundamentada en los principios de la seguridad de la información —confidencialidad, integridad y disponibilidad—, garantiza que los recursos informativos estén protegidos frente a amenazas y usos indebidos. Asimismo, la implementación de procesos de gestión del riesgo, que incluyen la clasificación de los tipos de riesgo y el desarrollo de fases estructuradas para su tratamiento, contribuye a anticipar, mitigar y controlar posibles incidentes. La integración de estas prácticas en un Sistema de Gestión de Seguridad de la Información (SGSI), respaldado por un marco normativo y orientado por un ciclo de mejora continua, fortalece la protección de los datos, optimiza la toma de decisiones y promueve una cultura organizacional orientada a la prevención y la confianza.

compuesto por

Nacional e internacional

PHVA

Media

Alta

se divide en

principios

contienen

abarcan

Baja

1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| **Nombre de la Actividad** | Reconocimiento de aspectos de inteligencia artificial generativa. |
| **Objetivo de la actividad** | Fortalecer los conocimientos relacionados con inteligencia artificial generativa, de acuerdo con los procedimientos del SGSI. |
| **Tipo de actividad sugerida** |  |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Actividad\_didactica\_CF01 |

1. **MATERIAL COMPLEMENTARIO:**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| 1. Activos de información | Departamento Nacional de Planeación (DNP). (2023). *Manual para la identificación de activos de información*. https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-13%20Manual%20para%20la%20identificación%20de%20activos%20de%20información.Pu.pdf | Documento | https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-13%20Manual%20para%20la%20identificación%20de%20activos%20de%20información.Pu.pdf |
| 1. Activos de información | Ministerio de Tecnologías de la Información y las Comunicaciones. (2024, 26 de diciembre). *Registro de Activos de Información*. https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135888:Registro-de-Activos-de-Informacion | Hojas de calculo | https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135888:Registro-de-Activos-de-Informacion |
| 1. Activos de información | Agencia Nacional Digital (AND). (2020). *Guía de gestión y clasificación de activos de información.* https://and.gov.co/sites/default/files/2022-05/Guia\_De\_Gestion\_y\_clasificacion\_de\_activos\_de\_informacon.pdf | Documento | https://and.gov.co/sites/default/files/2022-05/Guia\_De\_Gestion\_y\_clasificacion\_de\_activos\_de\_informacon.pdf |
| 3. Gestión de riesgo | Dirección de Impuestos y Aduanas Nacionales (DIAN). (2023). *Gestión de Riesgos de Seguridad de la Información.* <https://www.dian.gov.co/atencionciudadano/LMDP/Informacion-Innovacion-y-Tecnologia/Seguridad-de-la-Informacion/Cartillas/CT-IIT-0132.pdf> | Documento | https://www.dian.gov.co/atencionciudadano/LMDP/Informacion-Innovacion-y-Tecnologia/Seguridad-de-la-Informacion/Cartillas/CT-IIT-0132.pdf |
| 3. Gestión de riesgo | Departamento Nacional de Planeación (DNP). (2022, 26 de julio). *Módulo 1: Estructura del SGSI, riesgos de los activos y obligaciones de seguridad de la información* [Video]. YouTube. <https://www.youtube.com/watch?v=O3CwPYPzWzw> | Vídeo | https://www.youtube.com/watch?v=O3CwPYPzWzw |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Activos de información: | elementos que poseen valor para una organización, como datos, *software*, *hardware*, personas o servicios. Identificarlos y clasificarlos es fundamental para su protección dentro del sistema de seguridad. |
| CIA (Confidencialidad, Integridad, Disponibilidad): | principios fundamentales de la seguridad de la información, que aseguran que los datos sean accesibles solo por personas autorizadas, no sean alterados indebidamente y estén disponibles cuando se necesiten. |
| Ciberseguridad: | práctica enfocada en proteger sistemas informáticos y redes contra ataques digitales, amenazas maliciosas y accesos no autorizados que puedan comprometer la información de la organización. |
| Gestión de riesgos: | conjunto de procesos que permite identificar, analizar, valorar, tratar y monitorear riesgos, con el fin de minimizar su impacto en la seguridad de la información y los objetivos organizacionales. |
| Mejora continua: | proceso cíclico mediante el cual una organización evalúa y ajusta regularmente sus controles y políticas para adaptarse a nuevos riesgos y asegurar la eficacia del SGSI. |
| 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. |
| Políticas de seguridad: | directrices establecidas por una organización para proteger su información, definir responsabilidades y orientar el comportamiento de los empleados en relación con la gestión de datos. |
| Riesgo: | posibilidad de que una amenaza aproveche una vulnerabilidad para causar daño a los activos de información, afectando la confidencialidad, integridad o disponibilidad de los mismos. Su análisis permite tomar decisiones informadas. |
| 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. |
| Sistema de Gestión de Seguridad de la Información (SGSI): | marco estructurado que permite gestionar de forma efectiva la seguridad de la información, integrando políticas, controles, evaluaciones y acciones de mejora en toda la organización. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

GRCTools. (s.f.). *Riesgos IT y Seguridad con el Software GRC inteligente*. <https://grctools.software/soluciones/riesgos/riesgos-it-seguridad-de-la-informacion/>

Grupo Cibernos. (s.f.). *¿Qué es la gestión de riesgos en ciberseguridad?* <https://www.grupocibernos.com/blog/que-es-la-gestion-de-riesgos-en-ciberseguridad>

IBM. (2024a). *¿Qué es la seguridad de la información (InfoSec)?* <https://www.ibm.com/mx-es/topics/information-security>

IBM. (2024b). *¿Qué es la gestión de riesgos cibernéticos?* <https://www.ibm.com/es-es/topics/cyber-risk-management>

It Governance. (2022). *ISO 27005.* <https://www.itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005>

Kantan. (2024). *Definición de SGSI según ISO 27001 2022*. <https://www.kantansoftware.com/blog/definicion-de-sgsi-segun-iso-27001-2022/>

López, A. (2013). *SGSI. ISO 27000*.

Microsoft. (s.f.). *¿Qué es la seguridad de la información (InfoSec)?* <https://www.microsoft.com/es-co/security/business/security-101/what-is-information-security-infosec>

Novasep. (s.f.). *La seguridad de la información y sus 3 pilares fundamentales*. <https://www.novaseguridad.com.co/seguridad-de-la-informacion-principios/>

Rabitti, G., Khorrami Chokami, A., Coyle, P. & Cohen, R. D. (2025). A taxonomy of cyber risk taxonomies. *Risk Analysis An International Journal, 45*(2), 376–386. <https://doi.org/10.1111/risa.16629>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Armando Javier López Sierra | Experto temático | Regional Tolima. Centro de Comercio y Servicios. | Agosto de 2025 |
| Autor (es) | Andrés Felipe Velandia Espitia | Evaluador instruccional | Regional Tolima. Centro de Comercio y Servicios. | Agosto de 2025 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| Autor (es) |  |  |  |  |  |