Contexto, cronograma y diseño de estrategias de ciberseguridad

Breve descripción:

Mediante el desarrollo del presente componente el aprendiz estará en capacidad de comprender cómo realizar la implementación de una estrategia de seguridad a partir de procesos de planificación, que permita establecer las etapas y controles de seguridad y mejorar los niveles de seguridad de la organización.

Noviembre 2023

Tabla de contenido

Introducción

Para el proceso de implementación de una estrategia de gestión de la seguridad en una organización, se sugiere hacer uso y aplicación de la norma ISO/IEC 27001:2013, ya que esta norma brinda los lineamientos e instrucciones para su establecimiento. Además de presentar los fundamentos y aspectos más relevantes para su implementación, ofrece bajo su anexo A, un esquema de controles de seguridad, los cuales buscan abordar los aspectos más importantes para su adopción en el aseguramiento de los activos de información mediante el establecimiento de los objetivos de seguridad.

Le invitamos a hacer estudio de este componente formativo, activando todos los recursos didácticos que aquí se presentan, visitando los materiales complementarios que se le sugieren, analizando cada uno de los aspectos conceptuales y prácticos que se mostrarán y que darán línea al fortalecimiento de sus habilidades en la elaboración y aplicación de la estrategia de seguridad de información y ciberseguridad para su organización o empresa.

¡Adelante!

1. Determinar el contexto

En el ejercicio de implementación de estrategias de seguridad en las organizaciones, es conveniente conocer el contexto sobre el cual se realizarán las acciones que buscan el aseguramiento de los activos de información.

Este proceso permite:

- **Estimar**: valorar los activos
- **Valuar**: establecer el valor del riesgo presente
- **Dimensionar**: dimensionar los controles a utilizar
- **Identificar**: fijar los recursos y tiempo necesario para su implementación

1.1. Algunos conceptos y estándar orientador

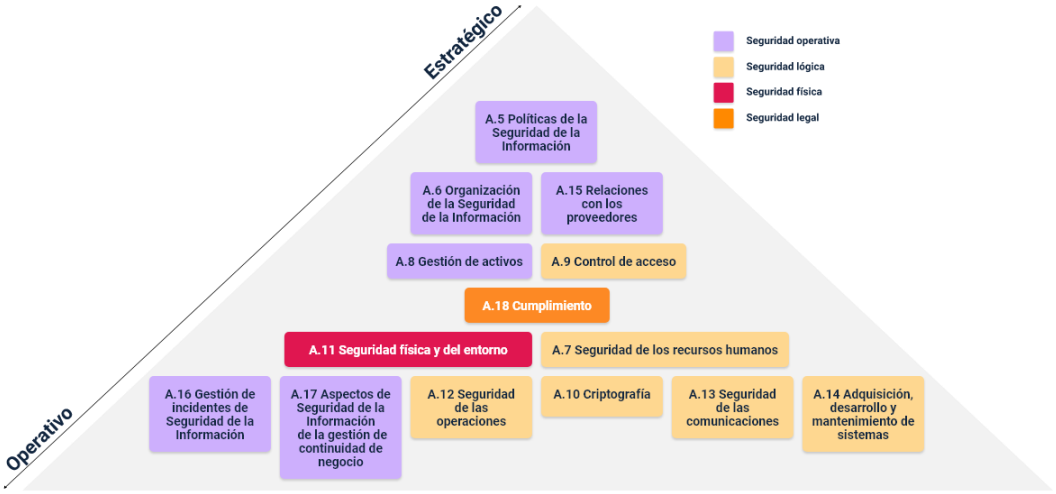
El estándar **ISO/IEC 27001:2013** presenta directrices para implementar SGSI en una organización. Esta se encuentra estructurada bajo el ciclo PHVA (planear, hacer, verificar, actuar) que permite llevar a cabo el proceso de implementación; en dicho ciclo se encuentra la fase de planeación, la cual cuenta con un elemento fundamental como es el análisis de riesgos, que permite reconocer el nivel de seguridad previo de los activos de información en una organización.

A partir de este análisis, se propone un plan de trabajo que involucra la determinación del plan de acción a desarrollar con el objetivo de reducir el riesgo en la organización.

Esta norma cuenta con el Anexo A en el cual se definen los Objetivos de Control y Controles de Referencia que permite identificar los controles de seguridad a implementar en la organización y esta se establece mediante el documento denominado Declaración de Aplicabilidad.

A continuación, se presentan algunos conceptos importantes a tener en cuenta en el ejercicio de la determinación del plan de trabajo para la implementación de la ciberseguridad.

Dominio de seguridad: se trata de la categoría o las categorías de seguridad que abordan los principales dominios a tener presentes en el establecimiento de la seguridad. La norma, actualmente, se encuentra estructurada por 14 dominios que representan los niveles de seguridad como son: operativos, lógicos, físicos y legales. Adicionalmente, estos niveles de seguridad, también se pueden identificar desde el ámbito estratégico y operativo



Nota: Adaptada de ISO/IEC 27001:2013 – Anexo A

Dominios de la norma ISO/IEC 27001:2013

1. **Seguridad operativa:**
    - A.16 Gestión de incidentes de seguridad de la información
    - A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio
    - A.7 Seguridad de los recursos humanos
    - A.8 Gestión de activos
    - A.6 Organización de la seguridad de la información
    - A.15 Relaciones Con Los Proveedores
    - A.5 Políticas de la seguridad de la información
2. **Seguridad Lógica**
    - A.12 Seguridad de las operaciones
    - A.10 Criptografía
    - A.13 Seguridad de las comunicaciones
    - A.14 Adquisición, desarrollo y mantenimiento de sistemas
    - A.9 Control de acceso
3. **Seguridad física**
    - A.11 Seguridad física y del entorno
4. **Seguridad legal**
    - A.18 Cumplimiento

Objetivo de control: cada uno de los dominios de seguridad que presenta la norma ISO/IEC 27001:2013, descritos anteriormente, se encuentra dividido en categorías. Estas categorías se denominan Objetivos de control, los cuales establecen

las intenciones y metas principales, de cada control de seguridad que será implementado y operado.

Control: en este ámbito y en relación con lo explicado hasta este punto, el control o los controles, son aquellas acciones que se deben implementar bajo un proceso o procedimiento que garantice el alcance de los objetivos o metas de seguridad que haya fijado la organización o empresa.

1.2. Objetivos de control y su estructura

La estructura de los objetivos de control tiene tres segmentos: el dominio, que abarca al objetivo y los controles; en segundo lugar, está el objetivo, que obedece a la intención o meta de la organización según en relación al dominio y, por último, el control o controles, que se establecen a partir del objetivo que los implica y del dominio que los contiene.

Ejemplo de la estructura de un control

- **Dominio. Ejemplo**: A5 - Política de seguridad
- **Objetivo de control. Ejemplo:** política de seguridad de la información
- **Dimensionar. Ejemplo:**
  - Documento de política de seguridad de la información.
  - Revisión de la política de seguridad de la información.

Nota: Adaptada de ISO/IEC 27001:2013 – Anexo A

2. Dominios de control

Los dominios de seguridad que propone esta norma: ISO/IEC 27001:2013, se encuentran estructurados de acuerdo a los componentes y elementos más relevantes para el mejoramiento de los activos de información.

En una organización se deben gestionar, entre otros tantos, los activos de información de manera segura y responsable; por ello la norma recomienda que se cuente con políticas claras que apoyen el ejercicio de identificación y aseguramiento de dichos activos de la información.

En la siguiente tabla, conozca los objetivos de control para la determinación de estas políticas. Le sugerimos tomar nota atenta de los aspectos más importantes de este punto.

Tabla 1. A5 Política para la seguridad de la información

A.5.1	Orientación de la Dirección para la Gestión de la Seguridad de la Información: brindar orientación y soporte, por parte de la Dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Política para la seguridad de la información.
A.5.1.2	Revisión de las políticas para la seguridad de la información

Nota: Norma ISO/IEC 27001:2013 – Anexo A

2.1. Objetivos de control para seguridad de la información

En términos de seguridad, uno de los factores más relevantes en una organización o empresa, es brindar las directrices para identificar y mantener seguros los activos de información.

Visualice el siguiente recurso y consulte allí los objetivos de control para la organización de la seguridad de la información.

a. **Organización Interna:** establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de información dentro de la organización:
    - Roles y responsabilidades para la seguridad de la información.
    - Separación de deberes
    - Contacto con las autoridades
    - Contacto con grupos de interés especiales
    - Seguridad de la información en la gestión de proyectos
b. **Dispositivos Móviles y Teletrabajo:** garantizar la seguridad del teletrabajo y el uso de dispositivos móviles:
    - Política para dispositivos móviles
    - Teletrabajo

2.2. Objetivos de control para el factor humano

Uno de los factores más débiles en seguridad será el factor humano. Según el instituto internacional de estudios en seguridad global “El error humano es la principal

causa de infracciones de datos y no los ciberdelincuentes. Es aquí donde las compañías deben revisar sus protocolos" (**INISEG, 2020).**

Para abordar estos factores humanos, la norma presenta los objetivos de control que usted podrá estudiar en el siguiente recurso:

Antes de asumir el empleo: asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos para los roles para los que se los consideran.

- Proceso de selección
- Términos y condiciones del empleo

Durante la vigencia del empleo: asegurarse de que los empleados y contratistas, tomen conciencia de sus responsabilidades en seguridad de la información.

- Responsabilidad de la dirección
- Toma de conciencia, educación y formación en la seguridad de la información
- Proceso disciplinario

Terminación o cambio de empleo: proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

- Responsabilidades en la terminación

2.3. Objetivos de control para la gestión de activos

La gestión de activos de información cobra vital importancia dado que estos deben de mantenerse identificados, clasificados y salvaguardados.

Estudie la siguiente tabla, y conozca los objetivos de control que establecen los controles necesarios para gestionar estos activos.

Tabla 2. A8 Gestión de activos

A.8.1	Responsabilidad por los activos: identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos
A.8.1.2	Propiedad de los activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	Devolución de activos
A.8.2	Clasificación de la información: asegurar que la información recibe un nivel adecuado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información
A.8.2.2	Etiquetado de la información
A.8.2.3	Manejo de activos
A.8.3	Manejo de medios: evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.
A.8.3.1	Gestión de medios removibles
A.8.3.2	Disposición de los medios
A.8.3.3	Transferencia de medios físicos

Nota: Norma ISO/IEC 27001:2013 – Anexo A

2.4. Controles de accesos

Otro factor importante es la restricción al acceso a los activos de información. Se trata de los controles para gestionar estos accesos, prevaleciendo siempre la confidencialidad, privacidad y disponibilidad del activo de información.

Visualice el recurso que a continuación se le presenta. En él encontrará aspectos de suma importancia respecto de los controles de accesos. Recuerde tomar nota atenta de los elementos más destacados.

a. **Requisito del negocio para el control de acceso:** limitar el acceso a información y a instalaciones de procesamiento de información:
    - Política de control de acceso
    - Acceso a redes y a servicios en red
b. **Gestión de acceso de usuarios:** asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a sistemas y servicios:
    - Registro y cancelación del registro de usuarios
    - Suministro de acceso de usuarios
    - Gestión de derechos de acceso privilegiado
    - Gestión de información de autenticación secreta de usuarios
    - Revisión de los derechos de acceso de usuarios
    - Retiro o ajuste de los derechos de acceso
c. **Responsabilidades de los usuarios:** hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación:
    - Uso de información de autenticación secreta
d. **Control de acceso a sistemas y aplicaciones:** evitar el acceso no autorizado a sistemas y aplicaciones:

- Restricciones de acceso a la información
- Procedimiento de ingreso seguro
- Sistema de gestión de contraseñas
- Uso de los programas utilitarios privilegiados
- Control de acceso a códigos fuente de programas

2.5. Controles criptográficos

Para proteger la información, de ser accedida por personas o sistemas no autorizados, se recomienda el uso de sistemas y técnicas de criptografía, con el fin adicional de garantizar la confidencialidad e integridad de los mismos.

En la tabla que le presentamos, usted puede encontrar los controles sugeridos por la norma.

Tabla 3. A10 Criptografía

A.10.1	Controles criptográficos: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos
A.10.1.2	Gestión de llaves

Nota: Norma ISO/IEC 27001:2013 – Anexo A

2.6. Controles y objetivos para el aseguramiento físico

Como buenas prácticas de seguridad, se recomienda reducir los riesgos asociados por daños directos o factores que puedan afectar los activos de información o el desarrollo de las operaciones en la organización.

Estos son los controles sugeridos para el aseguramiento físico, así como para el entorno, en donde se encuentran ubicados dichos activos.

Áreas seguras: prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información

- ✓ Perímetro de seguridad física
- ✓ Controles de acceso físico
- ✓ Seguridad de oficinas, recintos e instalaciones
- ✓ Protección contra amenazas externas y ambientales
- ✓ Trabajo en áreas seguras
- ✓ Áreas de despacho y carga

Equipos: prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización

- ✓ Ubicación y protección de los equipos
- ✓ Servicios de suministro
- ✓ Seguridad del Cableado
- ✓ Mantenimiento de equipos
- ✓ Retiro de activos
- ✓ Seguridad de los equipos fuera de las instalaciones
- ✓ Disposición segura o reutilización de equipos
- ✓ Equipos de usuario desatendido

- ✓ Política de escritorio limpio y pantalla limpia

Dominios de control, desde la norma ISO/IEC 27001:2013

Para completar y profundizar en el conocimiento de los Dominios de control, orientados por la norma ISO/IEC 27001:2013, le invitamos a visitar el Anexo_1_DominiosDeControl y estudiar las tablas de controles de los entornos de la organización, que allí se registran.

Enlace del documento

3. Alcance de los controles de seguridad

En el ejercicio para la determinación de los controles que se desean aplicar, es importante determinar el alcance de su implementación, es decir, la efectividad e impacto que puedan llegar a tener sobre los procesos, procedimientos, logro de objetivos y toda otra particularidad de las operaciones de la organización.

En otros términos, el alcance de la implementación de los controles, está directamente relacionado con el análisis de riesgos realizados a los activos de información, que busca mitigar dichos riesgos y evitar cualquier nivel de impacto negativo.

A continuación; allí encontrará información amplia e importantísima para el estudio del alcance de los controles de seguridad. Información que necesita para cumplir con los objetivos de este componente formativo. ¡Adelante!

Video 1. Alcance de los controles de seguridad

Enlace de reproducción del video

Síntesis del video: Alcance de los controles de seguridad
En este video se explora el alcance de la implementación de los controles de seguridad en la organización, está directamente relacionado con el análisis de riesgos realizados a los activos de información, que busca mitigar dichos riesgos y evitar cualquier nivel de impacto negativo. Cuando se habla de alcance, se está haciendo referencia, además, a la efectividad e impacto que puedan llegar a tener sobre los procesos, los procedimientos, el logro de objetivos y todas las operaciones de la organización.

Enfoque: el establecimiento de los controles debe estar enfocado en garantizar el normal funcionamiento de la organización; además, garantizar los niveles aceptables en la confidencialidad, integridad y disponibilidad de la información.

Determinación del alcance: para determinar el alcance, es importante contar con los detalles sobre los activos de información con el fin de determinar los controles necesarios; desde el enfoque del control se pueden enunciar los siguientes tipos:

- **Controles de Gestión:** buscan controlas los riesgos que afectan la organización en cuanto a su estructura y dinámica de trabajo.
- **Controles Técnicos:** se relacionan con factores tecnológicos, basados en software, hardware, controles técnicos, de seguridad perimetral o a las comunicaciones, entre otros.
- **Controles Operacionales:** buscan reducir los riesgos a partir de directrices o lineamientos para el desarrollo de actividades o funciones propias de la organización, de manera segura.
- **Controles de cumplimiento:** estos controles buscan mejorar el cumplimiento y adaptación, por parte de la organización, en el desarrollo de sus funciones o actividades.

Clasificación de los controles: así mismo, desde la finalidad del control, estos se pueden clasificar de la siguiente manera:

- **Controles disuasorios**: son aquellos que buscan prevenir a un atacante potencial.

- **Controles preventivos:** buscan minimizar la probabilidad de que un incidente se presente en la organización.
- **Controles de detección:** buscan identificar el momento más exacto de cuándo sucede un incidente.
- **Controles correctivos:** se establecen para dar solución una vez que se presente un incidente en la organización.

Aplicabilidad de los controles: una vez identificados y establecidos los controles a implementar en los procesos de la organización, estos deben declararse mediante un documento denominado **Declaración de Aplicabilidad** (Statement of Aplicability SoA) el cual ofrece un punto de partida sobre los controles.

Este documento es construido durante el establecimiento del sistema de gestión de la seguridad de la información, por lo que se considera un **documento de referencia**, tanto para la **implementación** de controles, así como para su **evaluación**.

Controles: orientaciones de la norma

Para afianzar sus conocimientos en Controles de seguridad, sugeridos por la norma, diríjase a Sistema de bibliotecas del SENA, http://biblioteca.sena.edu.co/. En el menú “Consulta bibliográfica” seleccione “Bases de datos” y encuentre en “Base de datos ICONTEC” la norma ISO/IEC 27001:2013, Anexo A.

Enlace del documento

4. Técnicas de planificación

El proceso de planificación para la implementación de la estrategia de seguridad debe abarcar una revisión y verificación del informe de análisis de riesgos que permita determinar, en primer lugar, los activos de información que se desean proteger en la organización, así como las amenazas a las cuales están expuestos; este ejercicio conlleva al establecimiento de los objetivos de seguridad con los cuales se busca garantizar una mejora considerable de los niveles de seguridad de los activos en la organización.

Estos son algunos elementos claves, que han de tenerse en cuenta en el proceso de la planificación:

a. **Activo de información:** un activo de información de acuerdo a la norma ISO/IEC 27001:2012 es “algo que una organización valora y por lo tanto debe proteger”.
b. **Objetivo de seguridad:** son objetivos que se plantean a partir de los resultados de la evaluación de riesgos y reflejan la medida en la que se alcanzan los niveles de protección de los activos de información, para determinar la eficacia de los controles implementados.
c. **Registro:** son evidencias o anotaciones relacionadas con el desarrollo y ejecución de un control, de acuerdo a lo propuesto.

d. **Recurso:** corresponde a los elementos o insumos necesarios para la implementación de un control y se convierte en un aspecto fundamental en el ejercicio de establecer las acciones a implementar.
e. **Métrica:** las métricas son instrumentos que permiten verificar el nivel de cumplimiento de un control de seguridad de acuerdo a lo esperado y propuesto en la estrategia de seguridad.

4.1. La planificación y los objetivos

La planificación de la estrategia de seguridad se debe realizar mediante la construcción de los objetivos de seguridad, estos se deben proponer a partir del análisis de riesgos, realizado a los activos de información y establecer las acciones que se deben adelantar para tratar los riesgos de seguridad. Con los objetivos se busca garantizar los pilares de la información.

Para el establecimiento de los objetivos de seguridad es importante tener presente aspectos como:

1. Los recursos que se necesitan para realizar la implementación.
2. La persona, área o dependencia responsable del cumplimiento del objetivo.
3. El método de evaluación, con el fin de identificar si el objetivo se está cumpliendo.
4. Además, debe tener presente que todo el ejercicio de la construcción y ejecución del objetivo de control debe estar documentado, así como:
   - Definir cada objetivo y su finalidad.

- Las evaluaciones y seguimiento a la ejecución y verificación del control verificando que este se cumpla.

4.2. Características de validación

De acuerdo a las características de la estrategia de seguridad y controles de información que se vayan a implementar en la organización, se deben establecer los objetivos de seguridad, los cuales deben contar con características que permitan validar si fueron, o no, cumplidos.

En consecuencia, con la norma ISO/IEC 27001:2013 en su numeral 6.2, los objetivos de seguridad deben presentar las siguientes características:

- Estar alineadas a la política de seguridad de la información.
- Se deben de poder medir
- Tener presente el contexto de la estrategia de seguridad, así como el resultado del ejercicio de valoración de riesgos.
- Estos deben ser informados a todos los interesados.
- Deben ser evaluados y actualizados de acuerdo a las necesidades.

Importante

Se debe conservar la información documentada sobre los objetivos de la seguridad de la información.

Tenga presente

En el momento de realizar la planificación para garantizar el alcance de los objetivos propuestos, en relaciona con la seguridad de la información, se debe tener presente:

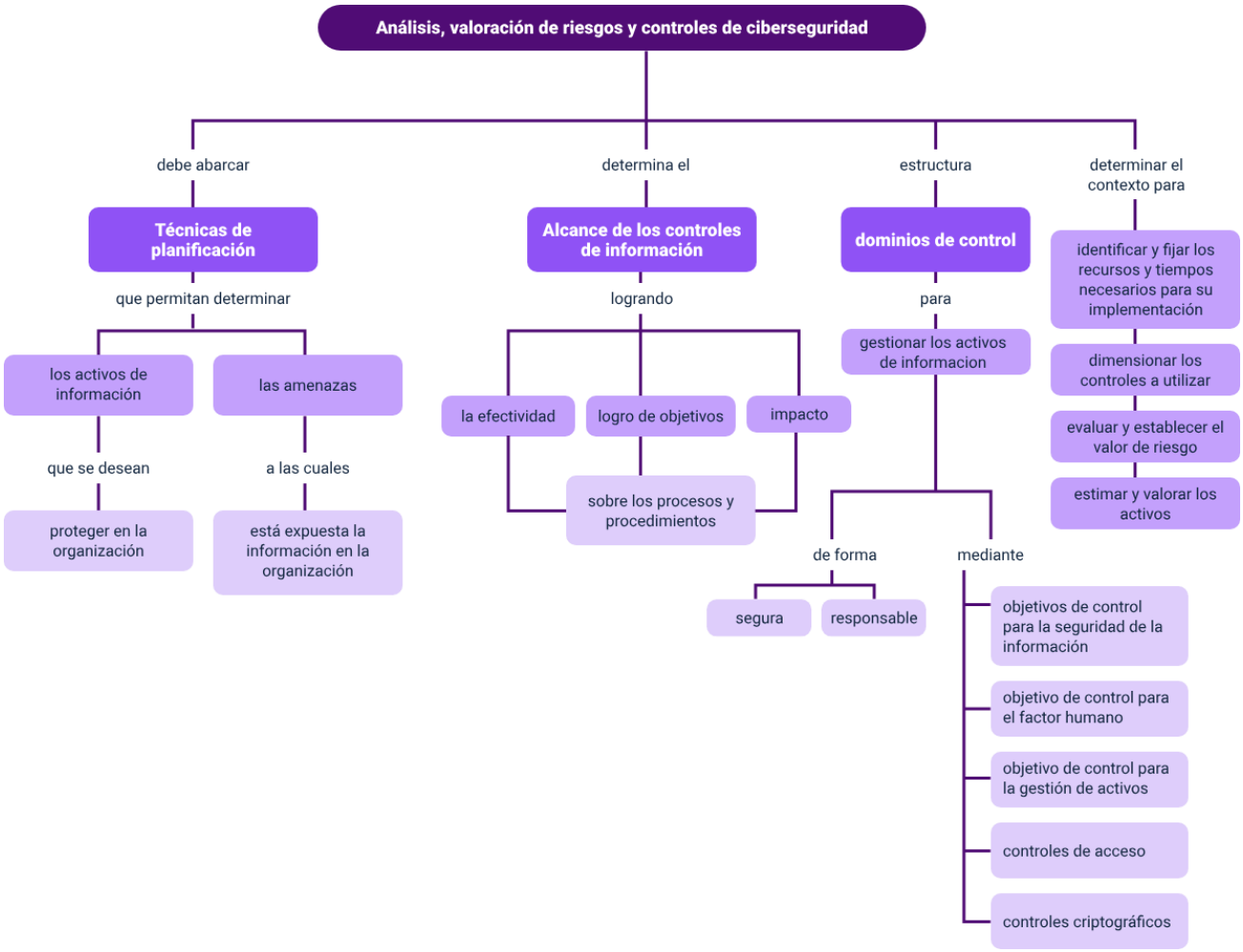
- ✓ Acciones a desarrollar
- ✓ Recursos necesarios
- ✓ Persona, área o dependencia responsable
- ✓ Tiempo necesario para culminar
- ✓ Método de evaluación

¡Atención!

La información documentada deberá ser conservada para su revisión en procesos de auditoría, tanto internas como externas, para cumplimiento y verificación.

Síntesis

Diseñar una estrategia de ciberseguridad efectiva es un proceso continuo y evolutivo, se debe tener en cuenta posibles amenazas que pueden surgir y las necesidades cambiantes de los activos de la información que se deseen proteger en la organización, esto es esencial para mantener un entorno digital seguro.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
3. Alcance de los controles de seguridad	ISO / IEC JTC 1 / SC 27 Seguridad de la información, ciberseguridad y protección de la privacidad. (2013). ISO / IEC 27001: 2013.	Norma técnica	https://www.iso.org/standard/54534.html

Glosario

Amenaza: es cualquier debilidad presente y que puede ser aprovechada para afectar un sistema de información.

Confidencialidad: principio con el cual, la información solo es accedida por la persona o sistema autorizado para su acceso.

Control: son acciones que se deben implementar bajo un proceso o procedimiento, para garantizar los objetivos de seguridad de la organización.

Disponibilidad: principio que supone que un activo de información se mantenga disponible sin sufrir ninguna degradación o alteración.

Integridad: principio que sugiere que la información se mantenga intacta y sin alteraciones posterior a sufrir un incidente.

Riesgo: probabilidad que suceda un incidente aprovechándose de una amenaza existente afectando los principios de la seguridad de la información.

Vulnerabilidad: falencia en un sistema que puede ser aprovechada para generar un incidente de seguridad.

Referencias bibliográficas

Instituto Internacional de Estudios en Seguridad Global (2020). Factor humano y ciberseguridad, un riesgo en crecimiento. INISEG. https://www.iniseg.es/blog/ciberseguridad/factor-humano-y-ciberseguridad/

Instituto Nacional de Tecnologías de la Comunicación (2009). Implantación de un SGSI en la empresa. https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO (2021). Dominios de seguridad y controles. (ISO 27000). https://www.iso27000.es/iso27002.html

ISO (2021). Planificación en ISO. (ISO 27001). https://normaiso27001.es/planificacion-en-iso-27001/

Organización Internacional de Normalización (ISO 2021). FASE 6 Implementando un SGSI. (ISO 27001). https://normaiso27001.es/fase-6-implementando-un-sgsi/

Créditos

Nombre	Cargo	Regional y Centro de Formación
Maria Camila Garcia Santamaria	Líder del equipo	Dirección General
Rafael Neftalí Lizcano Reyes	Asesor metodológico y pedagógico	Centro Industrial del Diseño y la Manufactura - Regional Santander
Hernando José Peña Hidalgo	Experto temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Fabián Leonardo Correa Díaz	Diseñador instruccional	Centro agropecuario La Granja - Regional Tolima
Carolina Coca Salazar	Revisora metodológica y pedagógica	Centro de Diseño y Metrología - Regional Distrito Capital
Jhana Johanna Bustillo Ardila	Revisión de estilo	Centro Industrial del Diseño y la Manufactura - Regional Santander
Francisco José Lizcano Reyes	Responsable del equipo	Centro Industrial del Diseño y la Manufactura - Regional Santander
Leyson Fabian Castaño Perez	Soporte organizacional	Centro de Comercio y Servicios - Regional Tolima
Luis Fernando Sarmiento Betancourth	Diseño web	Centro Industrial del Diseño y la Manufactura - Regional Santander
Gilberto Junior Rodríguez Rodríguez	Producción audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Lina Marcela Pérez Manchego	Producción audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Ludwyng Corzo García	Producción audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
María Carolina Tamayo López	Producción audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Producción audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Producción audiovisual	Centro de Comercio y Servicios - Regional Tolima
Lizeth Karina Manchego Suárez	Desarrollo front-end	Centro Industrial del Diseño y la Manufactura - Regional Santander
Andrés Mauricio Santaella Ochoa	Soporte front-end	Centro Industrial del Diseño y la Manufactura - Regional Santander
Yuli Marcela Gómez Tarazona	Validación de diseño y contenido	Centro Industrial del Diseño y la Manufactura - Regional Santander
Milady Tatiana Villamil Castellanos	Validación y vinculación en plataforma LMS	Centro de Comercio y Servicios - Regional Tolima