**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Tecnólogo en Implementación y operación de la Ciberseguridad |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501109. Diseñar el modelo de seguridad de la información de acuerdo  con estándares y marco de referencia. | RESULTADOS DE APRENDIZAJE | 220501109 – 1. Planificar el diseño de las estrategias de ciberseguridad según el plan de tratamientos y matriz de riesgos informáticos. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | CF 03 |
| NOMBRE DEL COMPONENTE FORMATIVO | 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. |
| PALABRAS CLAVE | Control, Cronograma, Dominio, Plan, Riesgo |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | Servicios |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

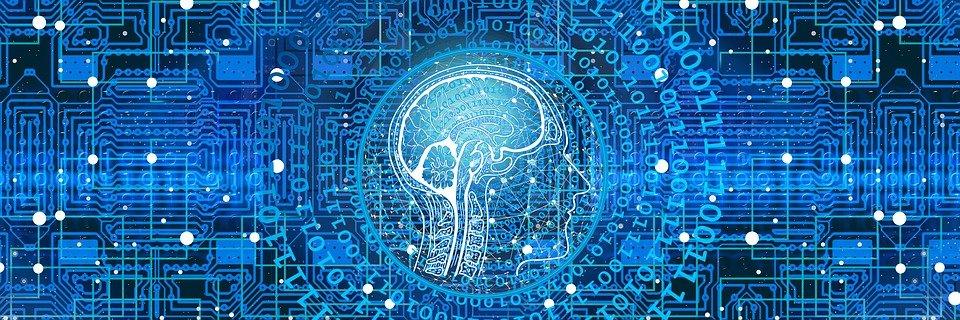
**Introducción**

* + - 1. **Determinar el contexto**
  1. **Algunos conceptos y estándares orientadores**
  2. **Objetivos de control y su estructura**

1. **Dominios de control**
   1. **Objetivos de control para la seguridad de la información**
   2. **Objetivos de control para el factor humano**
   3. **Objetivos de control para la gestión de activos**
   4. **Controles de accesos**
   5. **Controles criptográficos**
   6. **Controles y objetivos para el aseguramiento físico**
2. **Alcance de los controles de seguridad**
   1. **Determinación del alcance**
   2. **Calificación de los controles**
   3. **Aplicabilidad de los controles**
3. **Técnicas de planificación**
   1. **La planificación y los objetivos**
   2. **Características de validación**
4. **DESARROLLO DE CONTENIDOS:**

**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.



<https://cdn.pixabay.com/photo/2018/09/27/09/22/artificial-intelligence-3706562_960_720.jpg>

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.



<https://cdn.pixabay.com/photo/2020/05/18/16/17/social-media-5187243_960_720.png>

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. **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.



<https://media.istockphoto.com/vectors/grunge-green-iso-15378-certified-word-round-rubber-seal-stamp-on-vector-id1315960074?s=612x612>

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.

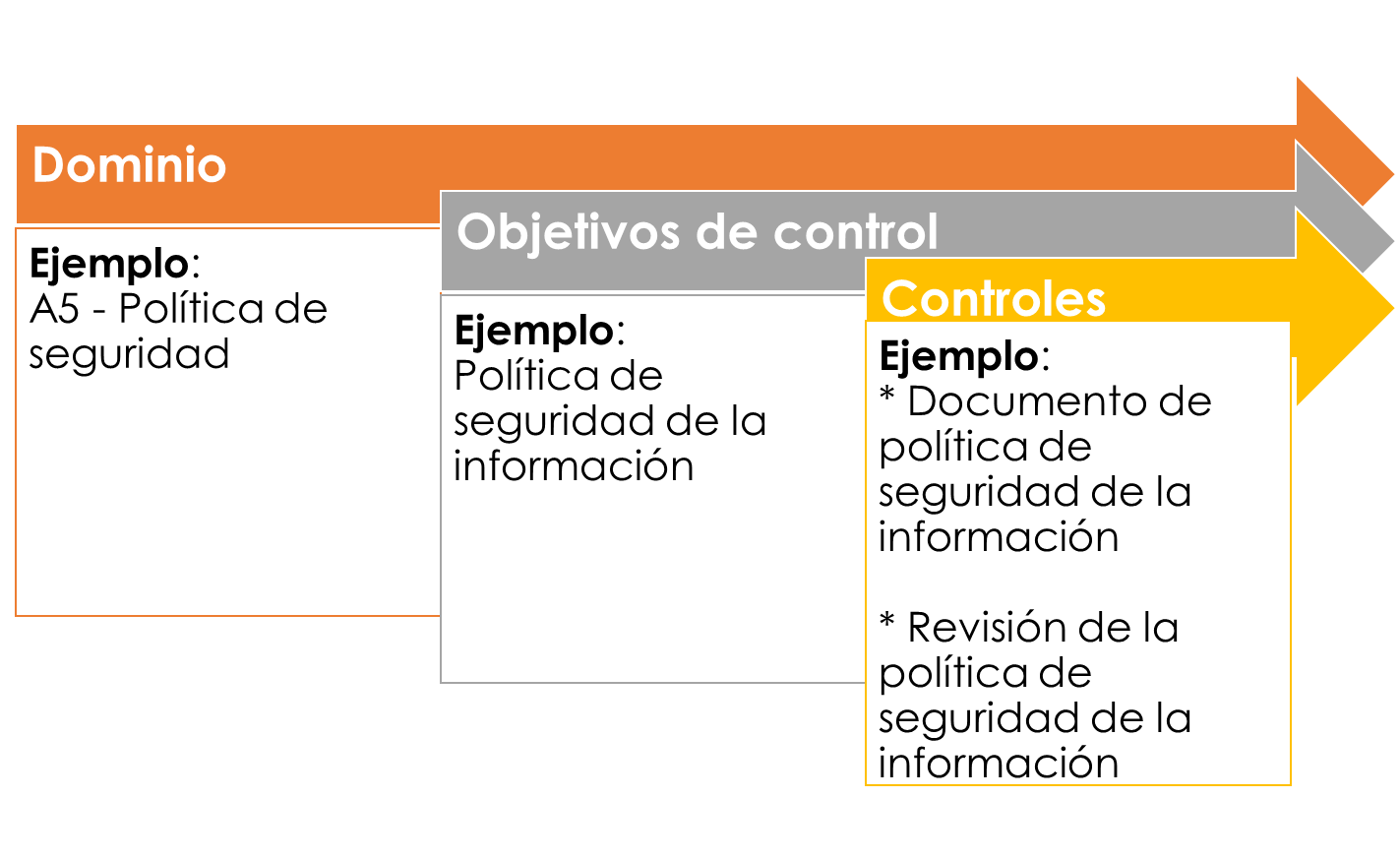
DI\_CF3\_1-1\_ConceptosYEstandarOrientador

* 1. **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.

***Figura 2.***

*Ejemplo de la estructura de un control*



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

1. **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.



<https://cdn.pixabay.com/photo/2018/01/17/04/14/industry-3087393_960_720.jpg>

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

* 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.**



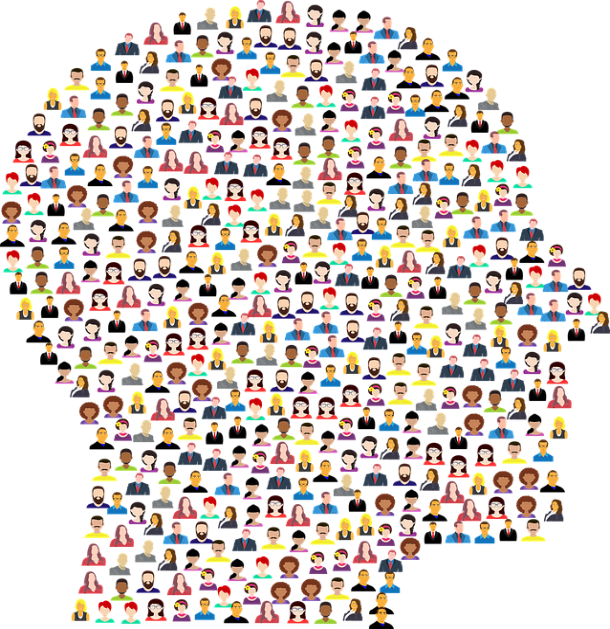
<https://cdn.pixabay.com/photo/2016/03/09/09/17/desktop-1245714_960_720.jpg>

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

DI\_CF3\_2-1\_ObjetivosControlSeguridadInformacion

* 1. **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).



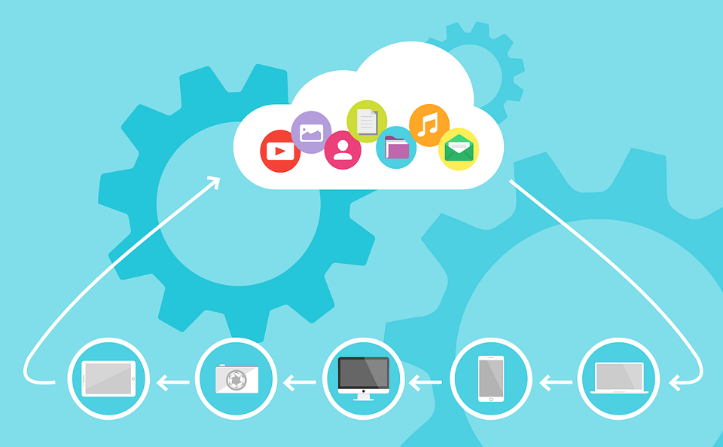
<https://cdn.pixabay.com/photo/2018/11/19/00/30/head-3824362_960_720.png>

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

DI\_CF3\_2-2\_ObjetivosControlFactorHumano

* 1. **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.



<https://cdn.pixabay.com/photo/2017/01/18/10/01/cloud-computing-1989339_960_720.png>

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

* 1. **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.



<https://cdn.pixabay.com/photo/2016/03/01/07/42/arrows-1229845_960_720.jpg>

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.

DI\_CF3\_2-4\_ControlesDeAccesos

* 1. **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

* 1. **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.



<https://cdn.pixabay.com/photo/2017/05/31/11/17/office-2360063_960_720.jpg>

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

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.

1. **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.

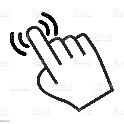


<https://cdn.pixabay.com/photo/2017/08/26/10/47/businessman-2682712_960_720.jpg>

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.

Diríjase al recurso que aparece 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**!

DI\_CF3\_3\_AlcanceControlesSeguridad



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.**

1. **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.



<https://cdn.pixabay.com/photo/2015/08/06/09/27/logistics-877568_960_720.jpg>

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

**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”.

**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.

**Registro**

Son evidencias o anotaciones relacionadas con el desarrollo y ejecución de un control, de acuerdo a lo propuesto.

**Recurso**

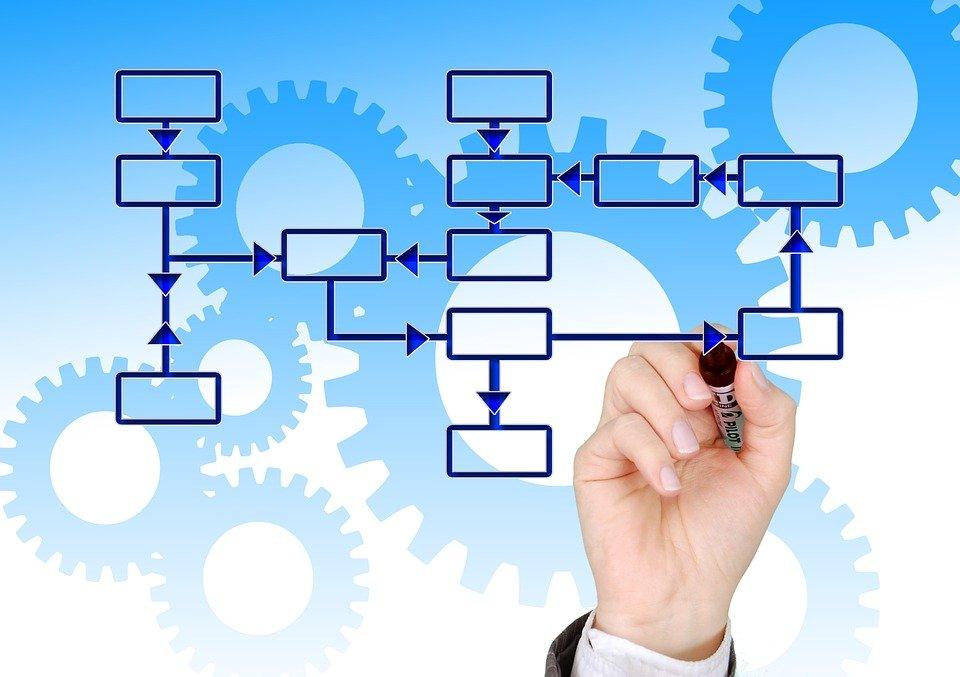
Corresponde a los elementos o insumos necesarios para la implementación de un control y se convierte en un aspecto fundamental en el ejercicio de establecer las acciones a implementar.

**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.

* 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.



<https://cdn.pixabay.com/photo/2015/10/19/07/38/mark-995567_960_720.jpg>

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

* Los recursos que se necesitan para realizar la implementación.
* La persona, área o dependencia responsable del cumplimiento del objetivo.
* El método de evaluación, con el fin de identificar si el objetivo se está cumpliendo.
* 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.
  1. **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.



<https://cdn.pixabay.com/photo/2016/12/07/09/27/fax-1889009_960_720.jpg>

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.

**C. SINTESIS**

Diseñar una estrategia de ciberseguridad efectiva es un proceso continuo y evolutivo, se debe adaptar a las amenazas en constante evolución y las necesidades cambiantes de los activos de la información que se deseen proteger en la organización, es esencial para mantener un entorno digital seguro.

**Escala de tiempo

Descripción generada automáticamente**

1. **ACTIVIDADES DIDÁCTICAS (OPCIONALES SI SON SUGERIDAS)**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Contexto y diseño de estrategias de ciberseguridad |
| Objetivo de la actividad | Apropiar conceptos requeridos para comprender el diseño de estrategias de ciberseguridad según matriz de riesgos informáticos. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | CF03­\_actividad\_didáctica |

**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 |
| 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*. <https://www.iso.org/standard/54534.html> | Otro: Norma técnica | <https://www.iso.org/standard/54534.html> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Amenaza | Una 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 de 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/>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Hernando José Peña Hidalgo | Experto Temático | Cauca - Centro de Teleinformática y Producción Industrial | Agosto 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Centro agropecuario La Granja, Regional Tolima | Agosto 2021 |
| Carolina Coca Salazar | Revisora metodológica y pedagógica | Regional Distrito Capital- Centro de Diseño y Metrología | Septiembre 2021 |

1. **CONTROL DE CAMBIOS**

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

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