**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 | 220501109-02 - Preparar las estrategias de ciberseguridad de acuerdo con la planificación del diseño realizado. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 04. |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Diseño y documentación de controles de ciberseguridad. |
| BREVE DESCRIPCIÓN | Mediante el estudio consciente de este componente, el aprendiz estará en capacidad suficiente para preparar las distintas estrategias de ciberseguridad y seguridad de la información, a la vez que podrá elaborar eficazmente la hoja de ruta, de acuerdo con los controles requeridos y los tipos de documentación. |
| PALABRAS CLAVE | controles, directrices, estándares, políticas, riesgos |

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

1. **Tabla de contenidos**

**Introducción**

* + - 1. **Diseño de controles de seguridad**
      2. **Pasos para el diseño de controles de seguridad**

2.1. Entradas y salidas

2.2. Actividades

2.3. Paso uno: identificación del estado actual

2.4. Paso dos: definición de los objetivos

2.5. Paso tres: determinación del estado deseado

2.6. Paso cuatro: determinación del nivel de riesgo aceptable

2.7. Paso cinco: definición y ejecución del plan de acción

* + - 1. **Controles: características**
      2. **Recomendaciones importantes sobre controles**
      3. **Documentación**
      4. **Generalidades de los activos de información**

1. **DESARROLLO DE CONTENIDOS**

**Introducción**

En la actualidad, la ciberseguridad y la seguridad de la información han adquirido gran importancia en las organizaciones, lo que conlleva que se desarrollen documentos y directrices que orienten el uso adecuado de tecnologías, favoreciendo así la relativa integridad tanto de la información como de las acciones y desarrollos que tiene lugar en el ciberespacio.



<https://cdn.pixabay.com/photo/2015/05/26/23/52/technology-785742_960_720.jpg>

**1. Diseño de controles de seguridad**

En este contexto de la ciberseguridad, se entiende por controles todas aquellas acciones, medidas o procesos que buscan asegurar el desarrollo normal del ciberespacio o del manejo de los equipos e información dentro de la organización.

El diseño de los controles ayuda a preparar las estrategias de ciberseguridad elaborando una hoja de ruta de acuerdo con normas y documentos requeridos ya establecidos.



<https://www.auditool.org/images/images/217810578.png>

Otros aspectos importantes de los controles de seguridad son:

**Madurez y capacidad de los sistemas**

Ayudan a trazar las estrategias para descubrir un camino que permita a la organización alcanzar el estado de madurez y capacidad deseado en todo lo que tiene que ver con seguridad digital.

**Responsabilidad del diseño de controles**

En la organización, quien se encarga de diseñar dichos controles es la oficina de Tecnologías de la Información (TI) o, en su defecto, una persona experta en seguridad que haya sido contratada para tal fin.

**Jefatura de sistemas**

En la mayoría de los casos, cuando la organización cuenta con la posibilidad de tener personal propio para esos propósitos, quien establece el diseño de controles es quien hace las veces de jefe o jefa de sistemas.

**2. Pasos para el diseño de controles de seguridad**

Para el estudio y profundización de los contenidos de este componente formativo, es importante una previa comprensión y adopción de la guía técnica denominada **G.ES.05** (sobre el diseño y las formas de ejecución e implementación de un plan de seguridad de la información), propuesta por **MinTIC**, con el fin de establecer dicho plan o estrategia.



<https://cdn.pixabay.com/photo/2018/11/16/14/29/papers-3819540_960_720.jpg>

A continuación, se muestran los pasos y requerimientos clave, indicados por la guía técnica G.ES.05. Se recomienda prestar mucha atención para comprenderlos, asimilarlos y tomar nota atenta de ellos:



**2.1. Entradas y salidas**

Se entiende como una entrada aquel o aquellos elementos ya existentes que serán de gran utilidad para instalar el paso. Se trata de elementos que ya tiene la organización en su haber y en su quehacer y que **favorecen la instauración de cualquiera de los cinco pasos** para cumplir con el diseño del plan de controles de seguridad.



<https://cdn.pixabay.com/photo/2015/03/30/12/42/network-698598_960_720.jpg>

En esta misma línea, están las **salidas**. Cuando se habla de salidas, se está haciendo referencia a las herramientas de registro o de documentación que se tendrán luego de haber analizado, ajustado o intervenido los documentos o registros ya existentes relacionados con objetivos, planes de acción, estados de ciberseguridad de la compañía o clasificación de los activos de información, entre otros.

**2.2. Actividades**

Los pasos que se siguen para el diseño de los controles de seguridad, además de estar estructurados y orientados por las **entradas** y las **salidas**, requieren el cumplimiento de algunas acciones o actividades, según el paso, que darán sentido, cumplimiento y efectividad a cada paso y, en consecuencia, a los controles.



<https://cdn.pixabay.com/photo/2018/03/30/22/05/teamwork-3276682_960_720.jpg>

El desarrollo de esas actividades deberá contemplar tiempos, responsables, herramientas, entradas y salidas de cada paso, propósitos de cada paso e intención de cada control.

**2.3. Paso uno: identificación del estado actual**

Este procedimiento es el primero de los pasos para el diseño de los controles de seguridad y está basado en la clasificación de los activos de información. Con este, se identifica el estado actual de capacidad o madurez que tiene el proceso de seguridad de la información en la organización.



<https://blog.smartekh.com/hs-fs/hubfs/QUE-ES-LA-TRIADA-DE-SEGURIDAD-O-CIA-TRIAD-Y-POR-QUE-DEBERIA--INTERESARTE.png?width=700&name=QUE-ES-LA-TRIADA-DE-SEGURIDAD-O-CIA-TRIAD-Y-POR-QUE-DEBERIA--INTERESARTE.png>

A continuación, la estructuración de este primer paso, con sus respectivas entradas, salidas y actividades:



**2.4. Paso dos: definición de los objetivos**

Se trata del segundo de los pasos para cumplir con el diseño de los controles de seguridad dentro de la organización y, con él, se han de tener en cuenta los objetivos establecidos para trazar e implementar la estrategia de seguridad de la información, con el debido cumplimiento de los criterios establecidos por la normativa. No olvide que la norma vigente y sobre la cual estamos haciendo énfasis en este componente formativo es la **ISO/IEC 27001-2013**.



<https://www.ttandem.com/media/aprende-a-definir-objetivos-medibles-para-tu-estrategia-de-marketing-digital-714x317.jpg>

Profundice en las entradas, salidas y actividades de este segundo paso en el recurso que, a continuación, se presenta:



**2.5. Paso tres: determinación del estado deseado**

Determinar el estado de seguridad que se desea alcanzar es el tercer paso que se sigue en el diseño de controles de seguridad. En este paso, hay que tener en cuenta el nivel del estado que se desea alcanzar con la aplicación y desarrollo de la estrategia de seguridad digital de la organización. Desde luego, este paso debe contemplar también el estado actual y partir de él.



<https://www.esan.edu.pe/apuntes-empresariales/2017/04/04/facebook-cualitativos-y-cuantitativos.jpg>

Entérese, a continuación, de las entradas, salidas y actividades que estructuran este tercer paso en el diseño de controles de seguridad:

**Entradas**

Algunas entradas para la determinación del estado deseado son: los objetivos de la estrategia de seguridad digital ya establecidos, el estado actual del proceso de seguridad digital y los estándares y/o mejores prácticas, como, por ejemplo, la **ISO 27001:2013** y la **ISO 27002:2013**.

**Salidas**

En la determinación del estado deseado, una salida necesaria es, justamente, la mirada al estado deseado. Ha de ser una herramienta organizada y en correspondencia lógica con el actual.

**Actividades**

**Determinar** el estado deseado del proceso de seguridad digital dentro de la organización, en términos cualitativos de atributos, resultados y características.

**Reconocer** el nivel de madurez deseado.

**Definir**, de la mano de la alta gerencia de la organización, el nivel de madurez deseado, determinando el proceso para que cumpla con sus objetivos y satisfaga las necesidades de la organización.



**2.6. Paso cuatro: determinación del nivel de riesgo aceptable**

Se trata del cuarto paso en el diseño de controles de seguridad y consiste en definir el nivel de riesgo máximo que la organización considera aceptable en lo referente a la seguridad digital. Este nivel de riesgo aceptable se tendrá en cuenta en la estrategia, con base en la necesidad de riesgo de la organización.



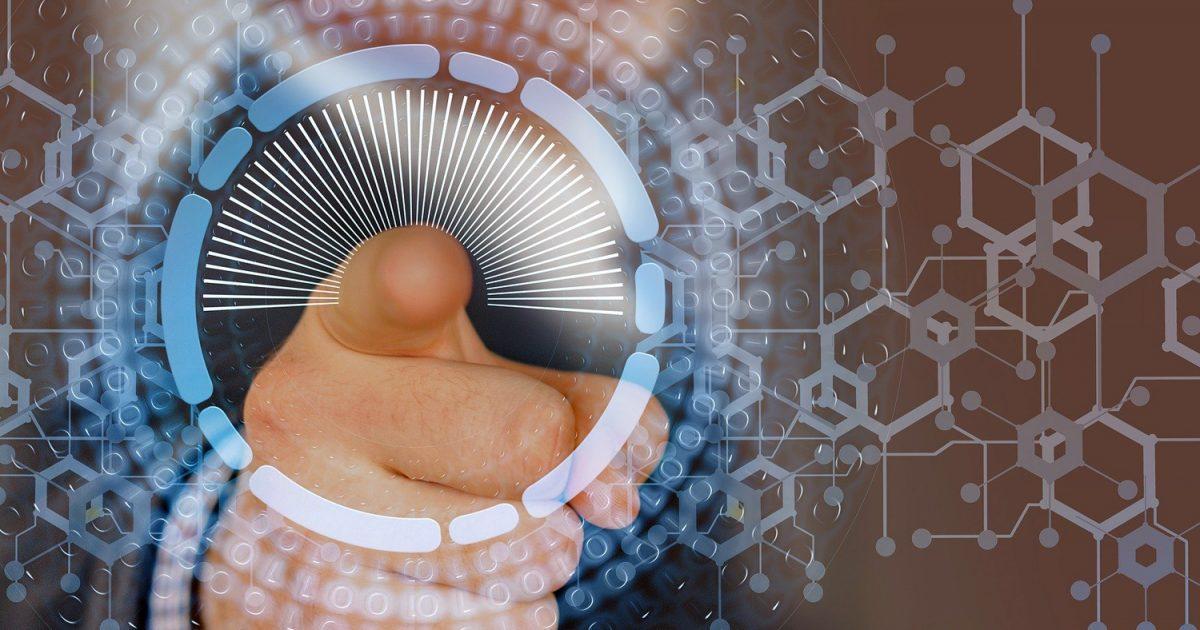
<https://www.teamnet.com.mx/hs-fs/hubfs/ORVZDV0%20(1).jpg?width=1500&name=ORVZDV0%20(1).jpg>



**2.7. Paso cinco: definición y ejecución del plan de acción**

Como quinto paso en el diseño de controles de seguridad, se encuentra la definición y ejecución del plan de acción. Se trata de fijar la hoja de ruta para lograr el estado deseado de la estrategia, teniendo en cuenta personas, tecnologías y procesos, entre otros recursos.



<https://www.segurilatam.com/wp-content/uploads/sites/5/2020/04/plan-director-de-seguridad-1200x630.jpg>

Se presentan ahora las entradas, salidas y actividades que estructuran el paso de definición y ejecución del plan de acción:



**3. Controles: características**

La estrategia de ciberseguridad y seguridad de la información de una organización ha de encaminarse y enfocarse en lograr la construcción de un ciberespacio seguro y resistente, que se alcanza, entre otras maneras, trazando las estrategias de acuerdo con los controles requeridos y, como se ha dicho ya, elaborando una hoja de ruta para mejorar el nivel de la ciberseguridad.



<https://cdn.pixabay.com/photo/2016/06/13/15/07/presentation-1454403_960_720.png>

En ese sentido, los controles de seguridad pueden caracterizarse con tres atributos constitutivos, que se presentan a continuación:

**Prevenir errores**

El carácter preventivo de los controles otorga al plan de seguridad un enfoque que favorece la intervención de los riesgos, antes de que estos se materialicen o, como es de esperarse, previniendo que estos sucedan con el mismo rigor y afectación que si no se previeran.



<https://media.istockphoto.com/vectors/cybersecurity-protection-network-safe-data-concept-web-page-design-vector-id1226870436?s=612x612>

**Detectar errores**

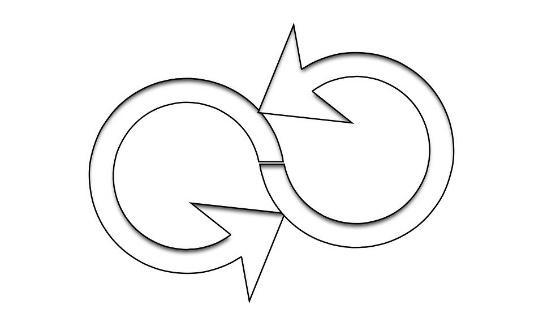
Detectar los errores es, básicamente, lograr ampliar el espectro de seguridad de los sistemas de información y, por tanto, generar con más acierto, en tiempo y forma, los mecanismos de intervención y atención a la materialización de los riesgos y/o errores detectados.



<https://cdn.pixabay.com/photo/2021/06/29/05/48/road-sign-6373274_960_720.jpg>

**Corregir errores**

La corrección de errores se presume como una acción necesaria cuando la prevención y la detección no han sido suficientes o no se han aplicado con el cuidado justo y pertinente. La corrección de los errores, siempre ofrecerá la posibilidad de generar mecanismos o acciones de prevención para nuevos riesgos o errores potenciales.



<https://cdn.pixabay.com/photo/2019/09/16/14/03/process-4481070_960_720.jpg>

**4. Recomendaciones importantes sobre controles**

Después de identificar el “**estado actual**” y el “**estado deseado**” del proceso de seguridad digital, se requiere analizar la brecha actual entre los dos estados, determinando la brecha por cerrar con la implementación de la estrategia.



<https://media.istockphoto.com/photos/hand-flip-wooden-cube-with-word-change-to-chance-self-improvement-picture-id1226916247>

Así, se requiere la ejecución de acciones complementarias que optimizarán los controles generados, como las que se sugieren en el siguiente listado:

* Disponer de planes de trabajo y proyectos para cerrar la brecha y así poder llegar al estado deseado.
* Acoger estándares de seguridad digital que soporten la política.
* Apoyar las acciones de la organización en las orientaciones de las normas técnicas existentes.
* Para este punto concreto, por ejemplo, se sugiere utilizar la ISO/IEC 27002:2013.
* Realizar un programa constante de sensibilización y capacitación en seguridad digital que posibilite implementar y adoptar, por todos los miembros de la organización, una estrategia eficaz.

1. **Documentación**

La documentación ha sido determinada por la FID (Federación Internacional de Información y Documentación) como “la colección, recopilación, almacenamiento, clasificación, selección, difusión, y utilización de todo tipo de información, cualquiera que sea su soporte”.

(EcuRed, s. f.)



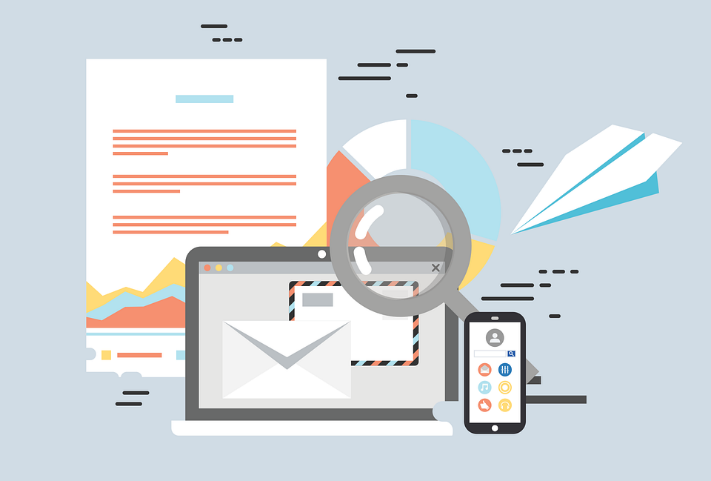
<https://media.istockphoto.com/photos/communication-network-concept-digital-transformation-picture-id1271635549?s=612x612>

En el recurso que se muestra a continuación, podrá profundizar en los aspectos fundamentales sobre procesamiento de la información en relación con la documentación que integra estos procesos:



1. **Generalidades de los activos de información**

Los activos de información relacionados con la seguridad de la información hacen referencia a cualquier información o dispositivo que tenga que ver con el tratamiento de ésta y que sea de valor para la organización.



<https://cdn.pixabay.com/photo/2019/06/19/07/13/email-4284157_960_720.png>

Los activos de información cuentan con un sistema de clasificación, el cual se enfoca en las propiedades de confidencialidad, integridad y disponibilidad como elementos para el tratamiento de los datos. Además, evalúa el impacto que se tendría en caso de no cumplir con alguno de estos fundamentos.

1. **Actividades didácticas (opcionales si son sugeridas)**

| Descripción de actividad didáctica | |
| --- | --- |
| Nombre de la actividad | N/A |
| Objetivo de la actividad |  |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (anexo donde se describe la actividad propuesta) |  |

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 |
| --- | --- | --- | --- |
| 2. Pasos para el diseño de controles de seguridad | Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2011). *Gestión del riesgo. Principios y directrices* (NTC-ISO 3100)*.* <http://simudatsalud-risaralda.co/normatividad_inv9/normas_tecnicas/NTC-ISO31000_Gestion_del_riesgo.pdf> | Norma técnica | <http://simudatsalud-risaralda.co/normatividad_inv9/normas_tecnicas/NTC-ISO31000_Gestion_del_riesgo.pdf> |
| 2. Pasos para el diseño de controles de seguridad | Organización Internacional de Normalización [ISO]. (2013). *Information Technology – Security Techniques – Code of Practices for Information Security Controls* (ISO 27002:2013). <https://www.iso.org/standard/54533.html> | Norma técnica | <https://www.iso.org/standard/54533.html> |
| 6. Generalidades de los activos de información | Organización Internacional de Normalización [ISO]. (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad.* (ISO 27001:2013) <https://www.iso.org/standard/54534.html> | Norma técnica | <https://www.iso.org/standard/54534.html> |

1. **Glosario**

| Término | Significado |
| --- | --- |
| Análisis de vulnerabilidades | Metodología por medio de la cual se valoran los sistemas y servicios de tecnología de la información en una organización y se comprueba la presencia de vulnerabilidades. |
| Contramedidas | Controles propios para riesgos específicos. |
| Control | Se trata de las acciones que se deben implementar bajo un proceso o procedimiento, para garantizar los objetivos de seguridad de la organización. |
| Directrices | Determinan las características generales de actuación. La directriz cuenta con un lineamiento normativo, lo que conlleva que sea general en su contenido y ámbito. |
| Entrada | Se trata de elementos que ya tiene la organización en su haber y en su quehacer y que favorecen la instauración de cualquiera de los cinco pasos para cumplir con el diseño del plan de controles de seguridad. |
| Integridad | Principio que sugiere que la información se mantenga intacta y sin alteraciones luego de sufrir un incidente. |
| Plan de acción | En el establecimiento de los controles de seguridad, el plan de acción se trata de la acción de fijar la hoja de ruta para lograr el estado deseado de la estrategia, teniendo en cuenta personas, tecnologías y procesos, entre otros recursos. |
| Riesgo | Toda posibilidad de sufrir una afectación por causa de factores externos o internos. El riesgo es un peligro latente que puede o no materializarse. En el orden informático y de ciberseguridad, los riesgos no son distintos, contemplan las vulnerabilidades y las amenazas y pueden ser controlados, tratados, mitigados, prevenidos y, en algunos casos, eliminados. |
| Salida | Herramientas de registro o de documentación que se tendrán luego de haber analizado, ajustado o intervenido los documentos o registros ya existentes, relacionados con objetivos, planes de acción, estados de ciberseguridad de la compañía o clasificación de los activos de información, entre otros. |

1. **Referencias bibliográficas**

Consejo Nacional de Política Económica y Social. (2011). *Lineamientos de políticas para Ciberseguridad y Ciberdefensa* (CONPES 3701). <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

EcuRed. (s. f.). *Documentación.* <https://www.ecured.cu/Documentaci%C3%B3n>

Ministerio de Hacienda y Administraciones Públicas. (2013). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>

Ministerio de Tecnologías de la Información y las Comunicaciones. (2011). *Modelo de Seguridad y Privacidad de la Información.* <https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf>

1. **Control del documento**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor(es) | Pablo Cesar Pardo Ortiz | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Agosto 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Tolima - Centro agropecuario La Granja | Agosto 2021 |
| Andrés Felipe Velandia Espitia | Revisor Metodológico y Pedagógico | Regional Distrito Capital – Centro de Diseño y Metrología | Septiembre 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor Pedagógico | Regional Santander –Centro Industrial del Diseño y la Manufactura | Septiembre 2021 |
| Darío González | Corrección de estilo | Regional Tolima – Centro Agropecuario La Granja | Septiembre 2021 |

1. **Control de cambios**

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