**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Implementación y operación de la ciberseguridad. |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | **220601044.** Monitorear sistemas de gestión de acuerdo con normativa y requerimientos técnicos. | RESULTADOS DE APRENDIZAJE | **220601044-1.** Proponer mejoras para la implementación de estrategias de ciberseguridad según los resultados de evaluación |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 11 |
| NOMBRE DEL COMPONENTE FORMATIVO | Mejoramiento continuo de las estrategias de ciberseguridad. |
| BREVE DESCRIPCIÓN | Mediante el estudio del presente componente, el aprendiz podrá identificar, explicar y aplicar aspectos fundamentales de la operación del ciclo de mejoramiento continuo de las estrategias de ciberseguridad en una organización, proceso fundamental para garantizar la actualización adecuada a las necesidades, a lo largo del tiempo. |
| PALABRAS CLAVE | Acciones, informe, mejoramiento, plan, revisión. |

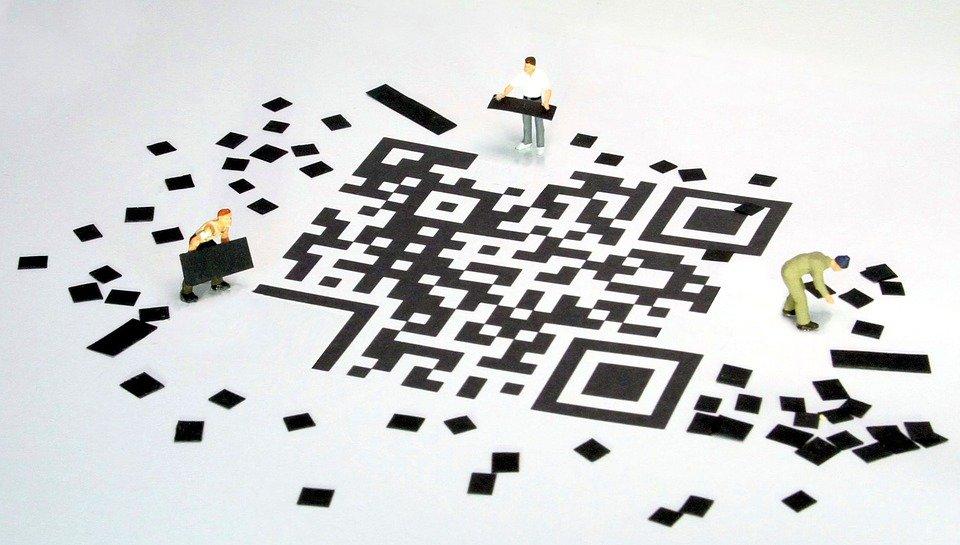
|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | **Servicios** |
| **IDIOMA** | **Español** |

1. **TABLA DE CONTENIDOS**

**Introducción**

1. **Análisis e interpretación de resultados**
   1. Actividades objeto de análisis
   2. Informe de auditoría
2. **Mejora continua**
3. **Normatividad corporativa de seguridad de la información**
4. **Buenas prácticas en ciberseguridad**
5. **DESARROLLO DE CONTENIDOS**

**Introducción**



<https://cdn.pixabay.com/photo/2019/02/02/14/27/qr-code-3970681_960_720.jpg>

Le damos la bienvenida al estudio de este componente. Para comenzar, revise el siguiente video, que aquí se muestra. ¡**Adelante**!

DI\_CF11\_0\_Introduccion\_formato\_4\_video

Para la elaboración de este componente, se abordaron varios autores conocidos en **mejoramiento continuo de las estrategias de ciberseguridad**, de quienes se han citado y referenciado conceptos y ejemplos para los fines educativos de este curso, en el entendido de que el conocimiento es social y, por lo tanto, es para ser usado por quienes necesitan adquirirlo. Se espera que este documento sea útil para todos aquellos, aprendices y lectores en general, que estén interesados en acercarse a asuntos básicos de la **implementación y operación de la ciberseguridad**.

1. **Análisis e interpretación de resultados**

En ciberseguridad, posterior a un proceso de evaluación de la seguridad digital, se debe realizar el **análisis y la interpretación** de resultados de evaluación, bien pueden ser resultados de auditorías, monitoreos o revisiones; esto permite plantear o proponer actividades de mejora, las cuales deben ser revisadas, aceptadas y ejecutadas por las partes responsables de las mismas.



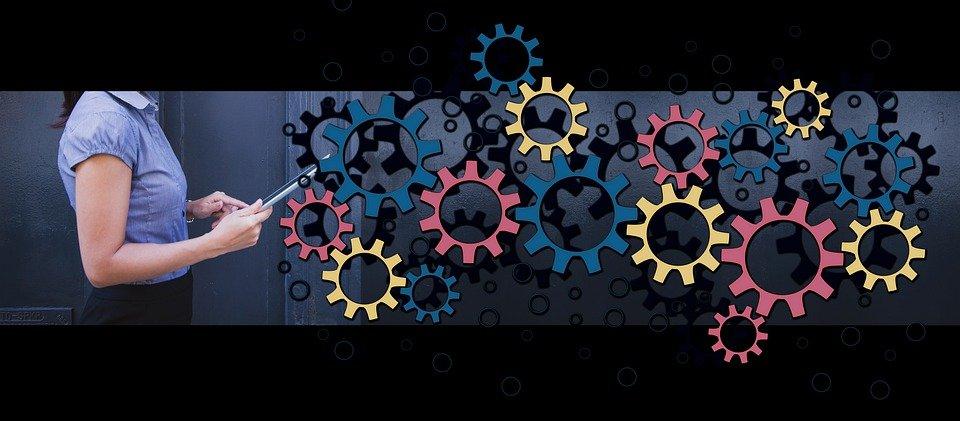
<https://cdn.pixabay.com/photo/2016/10/09/10/43/plan-1725510_960_720.jpg>

A continuación, una clave conceptual para diferenciar y comprender ambas acciones (análisis e interpretación):

DI\_CF11\_1\_Análisis\_e\_interpretación\_de\_resultados\_formato\_10\_tabs\_horizontales

* 1. **Actividades objeto de análisis**

Los análisis se hacen sobre resultados de evaluación realizados a procedimientos, actividades de proceso de seguridad digital o controles de ciberseguridad, así como a las auditorías de modelos de seguridad o sistemas de gestión de seguridad de la información.



<https://cdn.pixabay.com/photo/2019/11/23/05/00/business-4646286_960_720.jpg>

Las actividades objeto de análisis se pueden agrupar en *monitoreo de políticas y controles,* y en *auditorías de seguridad de la información y ciberseguridad.* Y, como se mostrará ahora, estos dos grupos tienen sus especificidades y particularidades importantes. ¡**Conózcalos**!

DI\_CF11\_1-1\_Actividades\_objeto\_de\_analisis\_formato\_11\_linea\_tiempo\_Vertical

* 1. **Informe de auditoría**

Consiste en un documento de informe donde se describen los aspectos de observaciones de mejora o no conformidades detectadas, según los objetivos y el alcance de un proceso de auditoría. El informe debe ser claro, conciso, constructivo y oportuno; su desarrollo debe ayudar a verificar el cumplimiento de sistemas, procesos, políticas, estándares, regulaciones, entre otros aspectos que se requieran revisar dentro una organización.



<https://cdn.pixabay.com/photo/2021/07/10/18/24/gears-6402028_960_720.jpg>

El informe de auditoría se convierte en un mecanismo objetivo para comunicar sobre las no conformidades y observaciones de mejora a las gerencias de áreas y alta gerencia dentro de una organización. Dichos informes deben ser precisos y detallados, de tal manera que se pueda informar sobre las fallas encontradas y sus respectivos soportes o evidencias.

La estructura base de un informe de auditoría cuenta con las siguientes partes:

* + Aspectos preliminares: propósito, objetivos, alcance de auditoría, métodos, enfoque.
  + Características generales: marco regulatorio y las características generales de la organización a evaluar.
  + Resultados de auditoría: no conformidades y observaciones de mejora encontradas.
  + Disposiciones finales: conclusiones y recomendaciones.

1. **Mejora continua**

La fase de mejora continua parte de la revisión a la evaluación de los indicadores de la estrategia de seguridad, generada por revisiones por parte de los responsables de procesos, la misma organización, auditorías internas o auditorías externas, estableciendo acciones que permitan corregir o mejorar sus capacidades para la gestión de la seguridad de la información.



<https://cdn.pixabay.com/photo/2020/05/22/12/14/business-5205180_960_720.jpg>

A continuación, se presenta una cita sobre mejora continua:

“*Lo que no se define no se puede medir. Lo que no se mide no se puede mejorar. Lo que no se mejora se degrada siempre*”.

**Lord Kelvin**

Partiendo de la premisa de Lord Kelvin, se puede abordar la fase de mejora continua como una **acción permanente de revisión y perfeccionamiento de los procesos de una entidad**. Esta fase debe contar con sus propios responsables, pero involucra a toda la organización y asegurará una buena gestión de la seguridad de la información. A continuación, se presentan algunos elementos que se deben precisar en los procesos de mejora continua.

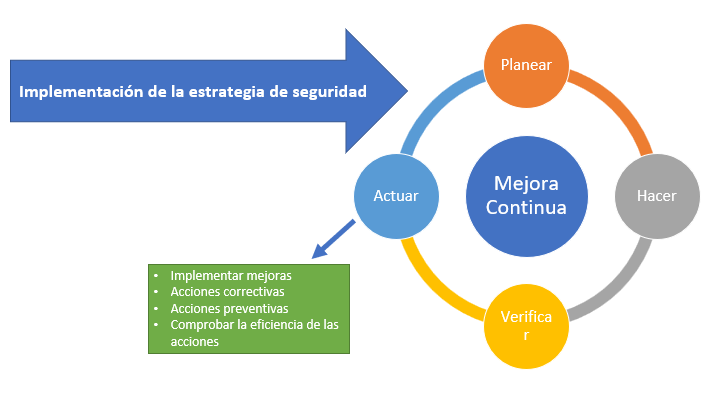
DI\_CF11\_2\_Procesos\_ de\_mejora\_continua\_formato\_6\_slide\_diapositivas\_simple

En síntesis y en palabras más puntuales, la mejora continua es el proceso mediante el cual, de manera sistemática, se mejoran los procesos y procedimientos relacionados con la estrategia de seguridad. Esto, a partir de la evaluación de los controles, políticas y documentos que permiten garantizar la seguridad de la información.

El proceso se debe de realizar permanentemente y de forma cíclica, permitiendo llevar un registro de las mejoras realizadas a la estrategia. Este concepto de mejora continua lo adoptan la mayoría de las normas de la familia ISO, lo cual facilita su implementación y el desarrollo de las acciones relacionadas. Ver Figura 1.

**Figura 1**

*Implementación de la estrategia de seguridad*



1. **Normatividad corporativa de seguridad de la información**

Desde una óptica corporativa, las organizaciones necesitan proceder en conformidad con los requerimientos, cumplimiento normativo y, como si fuera poco, mantenerse al margen de los riesgos a los que se ven enfrentadas día a día. Es por ello que han surgido iniciativas basadas en normas y estándares, que buscan apalancar el cumplimiento de dichas necesidades.



<https://cdn.pixabay.com/photo/2020/03/12/20/10/right-4926156_960_720.jpg>

El conocimiento amplio de los aspectos que las configuran y su aplicación son puntos clave que ayudan a garantizar la seguridad de la información y mediante los cuales se logra fortalecer el gobierno corporativo y su propuesta de valor frente a otras organizaciones.

Para reforzar su conocimiento sobre las normas que orientan las acciones enfocadas a la seguridad de la información, visite el **Anexo\_1\_NormativaSeguridadInformacion** y haga lectura consciente de la teoría allí contenida, fundamental para el avance satisfactorio en este componente.

1. **Buenas prácticas en ciberseguridad**

Un sistema de seguridad debe mejorarse de manera continua, y para ello, desde el área de seguridad, existen propuestas que facilitan la implementación de técnicas y tácticas de fortalecimiento de los activos de información.



<https://media.istockphoto.com/photos/businessman-using-tablet-and-laptop-analyzing-sales-data-and-economic-picture-id1165055244?s=612x612>

Conozca, ahora, algunas de las buenas prácticas más representativas:

DI\_CF11\_4\_Buenas\_practicas\_en\_ciberseguridad\_formato\_10\_tabs\_verticales(pasos)

Cada día, se unen más colaboradores a esta iniciativa, de la cual se puede obtener mayor información, que usted puede conocer en su portal: **https://www.cisecurity.org/cis-benchmarks/**

**Publicaciones especiales de NIST**

Desde NIST, *National Institute of Standards and Technology*, se vienen publicando una serie de documentos de apoyo a la gestión de la seguridad, bajo el prefijo SP (*Special Publication*), con los cuales se busca aportar desde algunas pautas a la estandarización de acciones que buscan mejorar la seguridad de los activos de información.



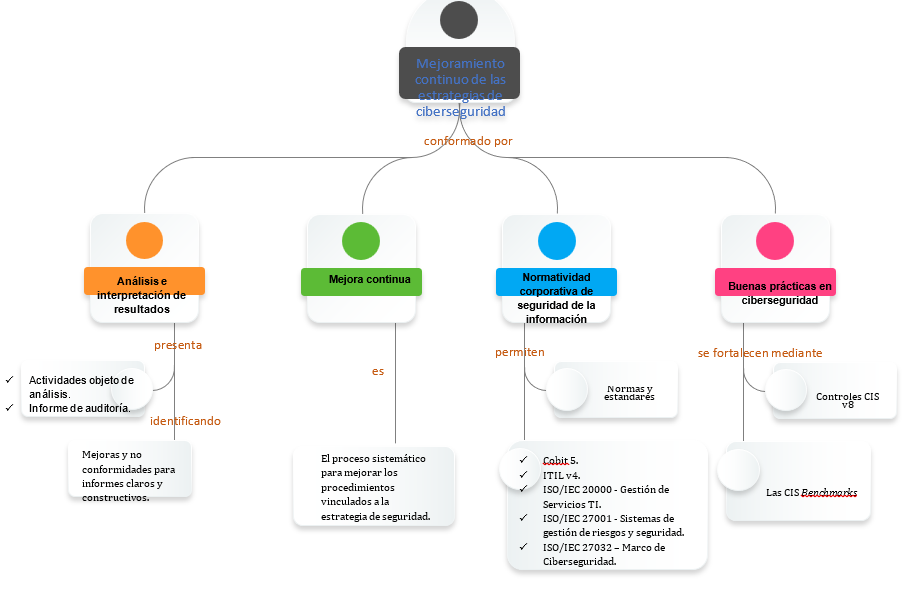
<https://cdn.pixabay.com/photo/2016/11/29/06/16/apple-1867752_960_720.jpg>

Entre las publicaciones más importantes, se encuentran aquellas relacionadas con auditorías, control del teletrabajo, control de dispositivos móviles, gestión de inventario de activos, entre otros, y algunos marcos de interoperabilidad.

Se sugiere que conozca estas publicaciones desde su sitio web: **https://csrc.nist.gov/publications/sp**

1. **SÍNTESIS**

En resumen, en el mejoramiento continuo de las estrategias de ciberseguridad, se abordaron aspectos cruciales, como el análisis detallado de vulnerabilidades, la evaluación de informes de auditoría, la implementación de mejoras constantes, el cumplimiento normativo corporativo y la adopción de buenas prácticas en ciberseguridad. Además, se utilizó la experiencia desde el NIST, Instituto Nacional de Normas y Tecnología**,** a través de sus publicaciones especializadas para aplicar principios avanzados de seguridad. Este enfoque integral garantiza la adaptación y fortaleza de las estrategias de ciberseguridad frente a las amenazas en constante evolución. A continuación, se presenta un mapa conceptual que resume la información de este proceso.



1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| Nombre de la actividad | Fortaleciendo la ciberseguridad: completando conceptos para el mejoramiento continuo |
| Objetivo de la actividad | Reconocer conceptos clave sobre el mejoramiento continuo de estrategias de ciberseguridad para fortalecer su comprensión práctica y habilidades de aplicación en entornos reales. |
| Tipo de actividad sugerida | Completar espacios |
| **Archivo de la actividad**  **(anexo donde se describe la actividad propuesta)** | Anexos/ DI\_CF11\_formato\_5\_actividad\_didactica\_completar\_espacios\_2023 |

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** |
| **4. Buenas prácticas en ciberseguridad** | South Security Cyber Community. (2021). *CIS Mapeo de Controles*. <https://www.southsecurity.org/resources/SouthSecurity-CIS_Mapeo_de_Controles.pdf> | Norma técnica | <https://www.southsecurity.org/resources/SouthSecurity-CIS_Mapeo_de_Controles.pdf> |
| **4. Buenas prácticas en ciberseguridad** | Center for Internet Security. (2021). *CIS Benchmarks*. CISECURITY. <https://www.cisecurity.org/cis-benchmarks/> | Norma técnica | <https://www.cisecurity.org/cis-benchmarks/> |

1. **GLOSARIO**

|  |  |
| --- | --- |
| **TÉRMINO** | **SIGNIFICADO** |
| **Ciberseguridad:** | conjunto de elementos articulados para la protección de la información alojados en dispositivos en el ciberespacio. |
| **Estándar:** | documento técnico que puede ser tomado como referencia para un caso específico. |
| ***Framework:*** | es un marco de trabajo específico, con instrucciones y estructuras, para la implementación de alguna acción. |
| **Incidente:** | suceso repentino no deseado. |
| **Norma:** | reglas organizadas y establecidas para la regulación de un comportamiento. |
| **Servicio:** | conjunto de herramientas y actividades que sirven para responder a una necesidad. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Center for Internet Security (2021). *CIS Benchmarks*. CISECURITY. <https://www.cisecurity.org/cis-benchmarks/>

ICONTEC. (2012). *Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información*. (GTC-ISO/IEC 27035). <https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=311>

ICONTEC. (2017). *Tecnología de la información. Gestión del servicio. Parte 2: código de práctica* (NTC-ISO/IEC 20000-2).<https://www.avancejuridico.com/docpdf/NORMA_TECNICA_20000-02.pdf>

ICONTEC. (2020). *Tecnologías de la información. Técnicas de seguridad. Directrices para ciberseguridad* (GTC-ISO-IEC 27032:2020). <https://tienda.icontec.org/gp-tecnologias-de-la-informacion-tecnicas-de-seguridad-directrices-para-ciberseguridad-gtc-iso-iec27032-2020.html>

ISO 27001. (s. f.-a). *Evaluación del Desempeño en ISO 27001- Requisitos en detalle*. <https://normaiso27001.es/evaluacion-del-desempeno-en-iso-27001/>

ISO 27001. (s. f.-b). *ISO 27001 Paso a Paso - 8 Auditoría Interna - ¿Cómo afrontarla?* <https://normaiso27001.es/fase-8-auditoria-interna-segun-iso-27001/>

ISO. (2020). *ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.* <https://www.iso.org/standard/54534.html>

Ministerio de Tecnologías de la Información y las Comunicaciones [Mintic]. (2016). *Guía de auditoría. Seguridad y privacidad de la información*. [https://www.mintic.gov.co/gestionti/615/articles-5482\_G15\_Auditoría.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf)

South Security Cyber Community. (2021). *CIS Mapeo de Controles*. <https://www.southsecurity.org/resources/SouthSecurity-CIS_Mapeo_de_Controles.pdf>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| **Autor (es)** | Hernando José Peña Hidalgo | Experto Temático | Cauca - Centro de Teleinformática y Producción Industrial | Septiembre de 2021 |
| Joaquín Patiño Cerón | Experto Temático | Cauca - Centro de Teleinformática y Producción Industrial | Septiembre de 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Centro agropecuario La Granja, Regional Tolima | Septiembre de 2021 |
|  | Darío González | Corrección de estilo | Regional Tolima - Centro Agropecuario La Granja | Octubre de 2021 |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del Cambio** |
| **Autor (es)** | Gloria Lida Alzate Suarez | Adecuador Instruccional | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
| Alix Cecilia Chinchilla Rueda | Metodología para la formación virtual | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de acuerdo con la directriz de Dirección General. |
| Liliana Victoria Morales Guadrón | Responsable Línea de Producción Distrito Capital. | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |