

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.

**Noviembre 2023**

Tabla de contenido

[Introducción 3](#_Toc152333011)

[1. Análisis e interpretación de resultados 5](#_Toc152333012)

[1.1. Actividades objeto de análisis 6](#_Toc152333013)

[1.2. Informe de auditoría 7](#_Toc152333014)

[2. Mejora continua 8](#_Toc152333015)

[3. Normatividad corporativa de seguridad de la información 12](#_Toc152333016)

[4. Buenas prácticas en ciberseguridad 13](#_Toc152333017)

[Síntesis 15](#_Toc152333018)

[Material complementario 16](#_Toc152333019)

[Glosario 17](#_Toc152333020)

[Referencias bibliográficas 18](#_Toc152333021)

[Créditos 19](#_Toc152333022)

Introducción

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

1. Mejoramiento continuo de las estrategias de ciberseguridad



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=pm9bgkdqRBg)

|  |
| --- |
| **Síntesis del video: Mejoramiento continuo de las estrategias de ciberseguridad** |
| La mejora continua es un proceso importante dentro de un sistema o modelo de seguridad de la información o ciberseguridad; esta permite la búsqueda constante del mejoramiento de procesos que hacen parte de una organización, minimizando errores y optimizando constantemente el desarrollo de las actividades. En ciberseguridad, las organizaciones y los gobiernos realizan esfuerzos para minimizar los riesgos, implementando controles de seguridad digital; dichos controles deben ser evaluados y mejorados continuamente para que cumplan con sus propósitos y no queden obsoletos o inadecuados en el tiempo. En este componente, se explorarán los elementos fundamentales para proponer estrategias y controles de seguridad digital, contribuyendo a la mejora constante de la ciberseguridad organizacional.  Recuerde:   1. Utilizar todos los recursos didácticos disponibles en este componente. 2. Llevar un registro de los conceptos teóricos y prácticos que aprende. 3. Disponer de un momento y lugar adecuados para estudiar este material. |

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.**

# 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.

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

1. **Análisis:** consiste en el proceso de estudiar los resultados obtenidos del proceso de evaluación de la ciberseguridad, buscando determinar qué fallas o debilidades se están presentando y deben ser corregidas o, también, los elementos que al respecto se deben mejorar.
2. **El análisis de resultados:** permite entender el panorama actual de ciberseguridad a través del estudio de los datos e información y tener una visión clara sobre las acciones adecuadas que se deben planificar y realizar para lograr mejorar los procesos de seguridad digital.
3. **Interpretación:** la interpretación de resultados de ciberseguridad está enfocada a determinar, a partir de resultados de evaluación de la seguridad digital, si se está cumpliendo con los objetivos y metas propuestos en los indicadores de gestión de la ciberseguridad o indicadores de seguridad digital. Esto permite dar a conocer a la alta gerencia o altos directivos sobre el estado de la ciberseguridad en la organización, a partir de resultados de evaluación.
4. **Interpretación objetiva:** las interpretaciones deben ser objetivas y conformes al contexto de la organización, de tal forma que se pueda dar a conocer, a las partes interesadas, los aspectos fuertes y aspectos por mejorar de la ciberseguridad, por medio de una comunicación clara y asertiva.

## 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.

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!**

1. **Monitoreo de políticas y controles:** consiste en las actividades de revisión del cumplimiento de políticas y controles de seguridad digital, donde se obtienen resultados para que, posteriormente, sean analizados y se logren determinar acciones para la mejora continua.
2. **Proceso interno:** el monitoreo de políticas y controles suele ser un proceso interno que es ejecutado por los equipos de seguridad al interior de las organizaciones, a los cuales les permite estar mejor preparados para procesos de revisión y auditoría tanto internas como externas.
3. **Auditorías de seguridad de la información y ciberseguridad:** consisten en revisión de aspectos de seguridad y ciberseguridad, con base en estándares o marcos de referencia, principalmente, los de ISO o NIST; tal es el caso de ISO/IEC 27001 o NIST “Cybersecurity Framework”.
4. **Procesos internos o externos:** las auditorías pueden darse de manera interna o externa, en la primera se busca el mejoramiento de los procesos internos en busca de la calidad. En las auditorías externas, las revisiones pueden realizarse con el fin de lograr un otorgamiento de calidad que dé un reconocimiento, el cual aumenta la imagen reputacional del proceso o de la organización.
5. **Solicitud de las auditorías:** además de ser solicitadas por la misma organización, las auditorías externas pueden presentarse por solicitud de entes regulatorios o de control, y su enfoque es revisar el cumplimiento legal de las organizaciones con las leyes vigentes.
6. **Resultados de las auditorías:** los resultados de evaluación de auditorías pueden arrojar no conformidades u observaciones de mejora, las cuales son importantes de analizar para la comprensión de las falencias de cumplimiento y los aspectos que se deben mejorar.

## 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.

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.

# 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.

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.

1. **No conformidad:** se le conoce como **no conformidad** al hallazgo por la falta o incumplimiento al desarrollo de un proceso y el cual no cumple con las condiciones esperadas de acuerdo con lo establecido en su propia estrategia de seguridad, poniendo en riesgo los pilares de la seguridad de la información.

Las no conformidades pueden ser detectadas a partir de auditorías, tanto internas como externas, o mediante procesos de monitoreo o mediciones de resultados. Cuando se trata de no conformidades detectadas por auditorías externas, las no conformidades se pueden catalogar como menores o mayores.

1. **No conformidades menores:** se trata de aquellas objeciones identificadas en la estrategia de seguridad, pero que no comprometen la integridad de la misma o del activo de información, y pueden ser abordadas con alguna acción correctiva en un tiempo estimado y, además, serán evaluadas en la próxima auditoría.
2. **No conformidades mayores:** son aquellas que sí ponen en riesgo, en principio, el funcionamiento de la estrategia de seguridad, y por ende afectan los pilares de la seguridad de la información, para los cuales también se deben establecer acciones correctivas con tiempo establecido, y se recomienda que sean revisadas antes de la siguiente auditoría.

Al identificar cualquier tipo de **no conformidad**, la organización puede, entre otras acciones, optar por:

* Controlar las inconsistencias y corregir las fallas.
* Asumir las consecuencias.
* Evaluar las causas que generaron la no conformidad, para eliminarla.
* Implementar acciones correctivas para subsanar las causas.
* Evaluar la eficacia de los controles y acciones implementadas.
* Evaluar la estrategia de seguridad para actualizarla, en caso de ser necesario.

1. **Acciones correctivas:** estas acciones permiten corregir o eliminar la causa que puede generar una **no conformidad**. Las acciones correctivas deben proponerse a partir de la identificación y deben ser evaluadas y aprobadas por la dirección y por el auditor que realizó la identificación de la no conformidad.

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. Revisar la siguiente figura.

1. Implementación de la estrategia de seguridad

Figura que muestra un diagrama de implementación de la estrategia de seguridad, el cual consta de: 

Mejora continua:
Planear
Hacer
Verificar
Actuar

# 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.

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.

**Normativa de la seguridad de la información**. Ver documento anexo **Normativa de la seguridad de la información**, ubicado en la carpeta de anexos, con la finalidad de reforzar su conocimiento sobre las normas que orientan las acciones enfocadas a la seguridad de la información.

# 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.

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

1. **Controles CIS v8:** los controles CIS son una propuesta de controles de seguridad específicos y con los cuales se busca endurecer las acciones defensivas y así prevenir incidentes que afecten los activos de información.
2. **En qué se basan los controles CIS v8:** esta propuesta está basada en múltiples marcos de seguridad, lo que permite abordar diferentes puntos de vista y, asimismo, recoger las mejores propuestas de seguridad.
3. **Estructuración de CIS v8:** los controles CIS están estructurados en 18 controles y 153 salvaguardas, distribuidos en 3 grupos de implementación.
4. **CIS “Benchmarks”:** esta otra iniciativa de recomendaciones específicas para productos de diferentes proveedores y tipos recopila una serie de recomendaciones y pautas para el endurecimiento de sistemas y aplicaciones, y así poder cumplir con un nivel básico de seguridad.
5. **Las más comunes:** entre las guías más comunes, se encuentran: sistemas operativos Linux y Windows, servicios web, bases de datos, hipervisores, servicios en la nube, dispositivos móviles, dispositivos de red, “software” de escritorio, dispositivos de impresión.

**Información CIS**

Cada día, se unen más colaboradores a esta iniciativa, de la cual se puede obtener mayor información, que usted puede conocer en su portal **Cisecurity.org.**

[**Enlace de la página web**](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.

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.

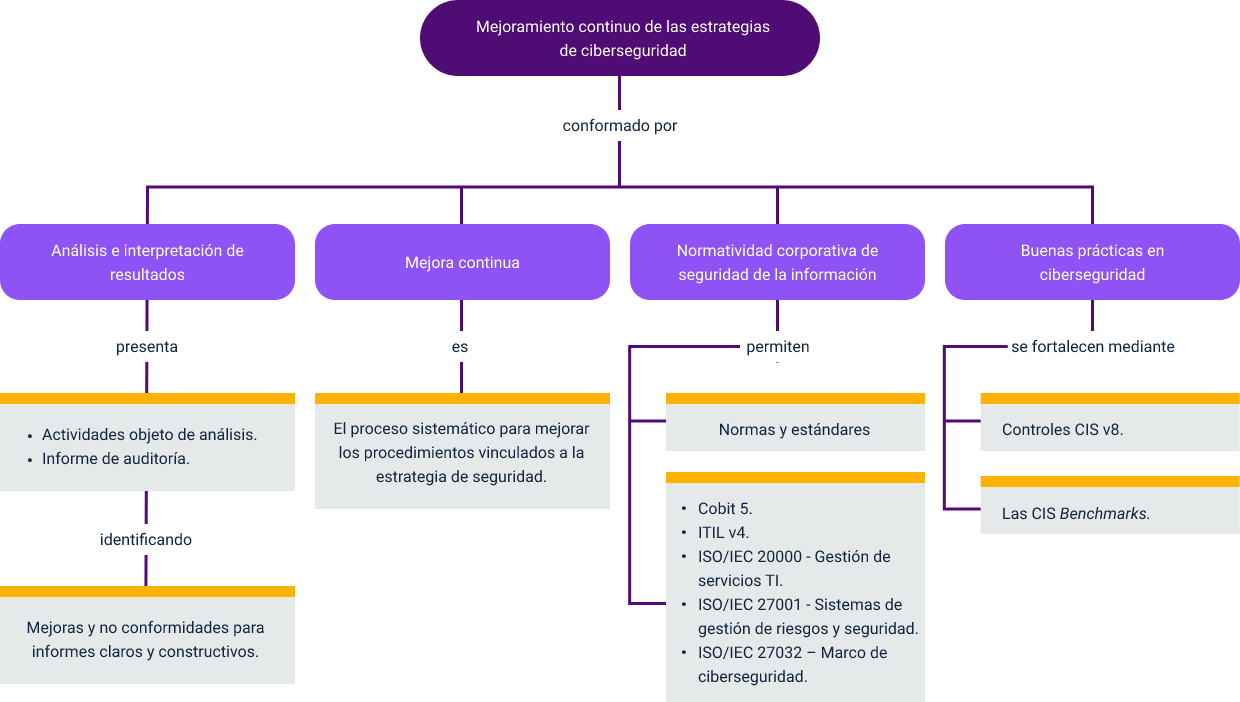
**Publicaciones de NIST**

Se sugiere que conozca estas publicaciones desde su sitio web:

[**Enlace de la página web**](https://csrc.nist.gov/publications/sp)

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.



Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| 4. Buenas prácticas en ciberseguridad | Center for Internet Security. (2023). *CIS Critical Security Controls v8 Mapping to NIST CSF*. | Norma técnica | <https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf> |
| 4. Buenas prácticas en ciberseguridad | Center for Internet Security. (2021). *CIS Benchmarks*. CISECURITY. | Norma técnica | <https://www.cisecurity.org/cis-benchmarks/> |

Glosario

**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.

Referencias bibliográficas

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

Center for Internet Security. (2023). *CIS Critical Security Controls v8 Mapping to NIST CSF*. <https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf>

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

ISO 27001. (s.f.). *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_Auditoria.pdf>

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| Claudia Patricia Aristizábal Gutiérrez | Responsable del equipo | Dirección General |
| Liliana Victoria Morales Gualdrón | Responsable de línea de producción | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Rafael Neftalí Lizcano Reyes | Asesoría metodológica y pedagógica | Regional Santander - Centro Industrial del Diseño y la Manufactura |
| Hernando José Peña Hidalgo | Experto temático | Regional Cauca - Centro de Teleinformática y Producción Industrial |
| Joaquín Patiño Cerón | Experto temático | Regional Cauca - Centro de Teleinformática y Producción Industrial |
| Fabián Leonardo Correa Díaz | Diseño instruccional | Regional Tolima - Centro agropecuario La Granja |
| Darío González | Corrección de estilo | Regional Tolima - Centro Agropecuario La Granja |
| Gloria Lida Alzate Suarez | Adecuación instruccional | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Alix Cecilia Chinchilla Rueda | Metodología para la formación virtual | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Yazmin Rocio Figueroa Pacheco | Diseño web | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Luis Jesús Pérez Madariaga | Desarrollo Fullstack | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Ernesto Navarro Jaimes | Animación y Producción audiovisual | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Lady Adriana Ariza Luque | Animación y Producción audiovisual | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Laura Gisselle Murcia Pardo | Animación y Producción audiovisual | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Carolina Coca Salazar | Evaluación de contenidos inclusivos y accesibles | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Lina Marcela Pérez Manchego | Validación de recursos educativos digitales | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Leyson Fabián Castaño Pérez | Validación de recursos educativos digitales y vinculación LMS | Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información |