**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

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

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501110 -Implementar el sistema de seguridad de la información según modelo y estándares técnicos. | RESULTADOS DE APRENDIZAJE | 220501110-2. Aplicar las estrategias de ciberseguridad conforme a la planificación realizada. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 06 |
| NOMBRE DEL COMPONENTE FORMATIVO | Aplicación de estrategias de ciberseguridad |
| BREVE DESCRIPCIÓN | Con el estudio de este componente el aprendiz estará más y mejor capacitado en el reconocimiento y aplicación de las técnicas y herramientas especializadas de gestión de la seguridad. Podrá afianzar sus conocimientos y habilidades en la implementación de controles y estrategias que garantizan la estabilidad de los pilares de la información en las organizaciones. |
| PALABRAS CLAVE | Auditoría, control, endurecimiento, privilegio, registro. |

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

1. **Tabla de contenidos**

**Introducción**

1. **Gestión de acceso**
   1. Pasos técnicos de la gestión de acceso
   2. Tipos de control para gestión de accesos
   3. Características
2. ***Firewalls***
3. **Sistemas de detección y prevención de intrusos IDS/IPS**
   1. Características funcionales de los IDS
   2. Características de los IPS
4. **Gestión unificada de amenazas UTM/XTM**
5. ***Antimalware***
6. **Detección y respuesta para *endpoints* (EDR)**
   1. Aspectos clave de los EDR
   2. Tipos de soluciones de seguridad para *endpoint*
   3. Características de las soluciones de seguridad
7. **Cifrado**
8. **Fuga de información**
   1. Prevención
   2. Recomendaciones para las organizaciones
9. **Dispositivos móviles**
   1. Riesgos asociados
   2. Controles
10. **GuíaNIST-SP800-114**
    1. Aspectos importantes de la guía
    2. Seguridad en el teletrabajo
11. **Infraestructuras críticas**
12. **Mejoras de ciberseguridad en infraestructuras**
13. **Sistemas de correlacionamiento de *logs* y monitoreo**
14. **Gestión de eventos e información de seguridad SIEM**
15. **Parcheado y/o actualización**
16. **Desarrollo de contenidos**

**Introducción**

En el ejercicio de implementación de las estrategias de seguridad se debe partir de los objetivos de seguridad propuestos, así como de la declaración de privacidad, lo cual indica los controles que habrían de ser adoptados en la organización y con ello, garantizar la seguridad de la información.



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

En este componente formativo podrá hacer un recorrido por algunas técnicas y herramientas, según el modelo y los estándares técnicos, que respondan de manera pertinente a la planificación en su organización, a la vez que profundiza en ellas.

1. **Gestión de acceso**

Actualmente, la información se considera uno de los activos más importantes para las organizaciones, debe contar con mecanismos que garanticen que, únicamente las personas autorizadas puedan acceder y realizar las acciones pertinentes y asociadas a sus funciones.

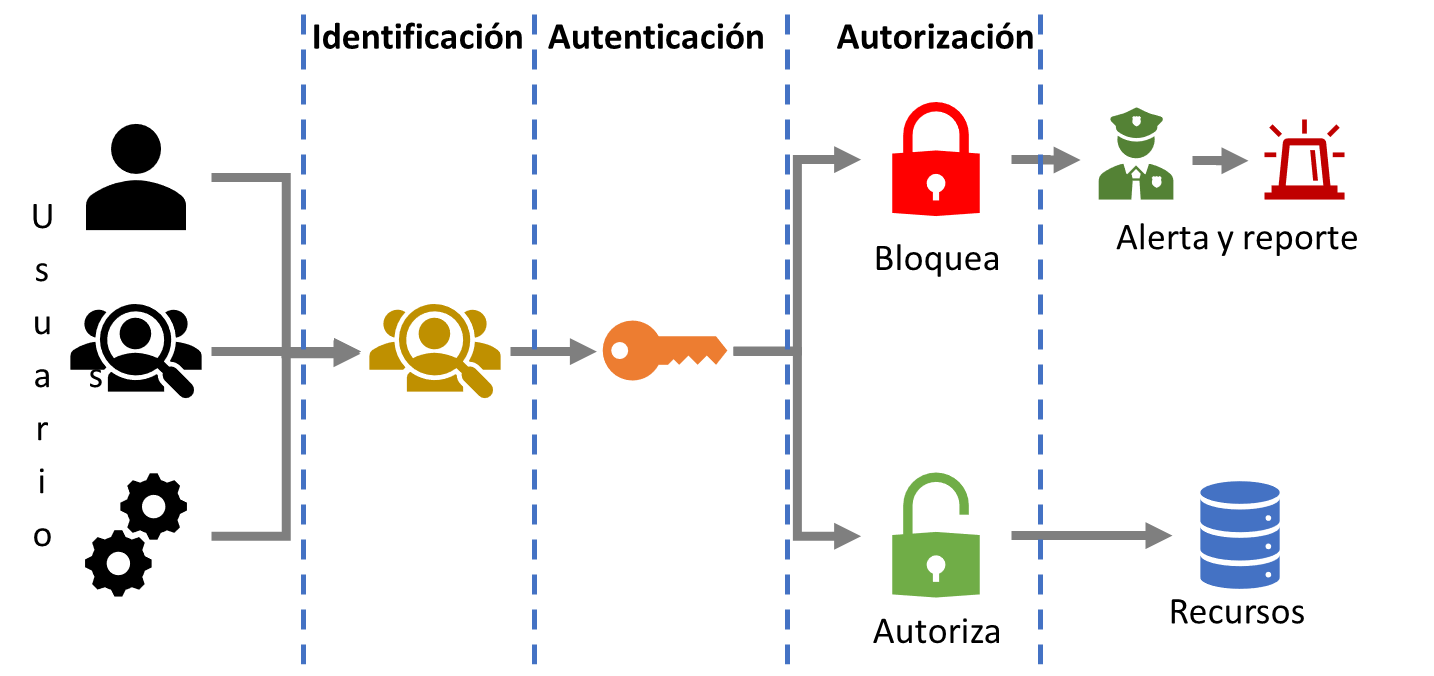
<https://cdn.pixabay.com/photo/2017/10/30/18/44/hacking-2903156_960_720.jpg>

* 1. **Pasos técnicos de la gestión de acceso**

De acuerdo con el Instituto Nacional de Ciberseguridad de España un objetivo de este control es “establecer quién, cómo y cuándo puede acceder a los activos de información de la empresa y registrar convenientemente dichos accesos” (Incibe, 2017); esto indica el establecimiento de controles que permitan una adecuada gestión de los permisos de los usuarios u otros sistemas de información para interactuar con los activos de una organización. En la siguiente figura, se pueden observar los pasos que se llevan a cabo para el control de gestión de acceso.

**Figura 1.**

*Pasos de un control de gestión de acceso*



Nota. Adaptado de ICHI.PRO - Introducción a la gestión de identidades y accesos.

Durante el acceso a los sistemas de información se deben llevar a cabo una serie de **pasos técnicos,** los cuales deben valorarse para gestionar una adecuada autorización y acceso a los recursos requeridos; a saber:

**Identificación**

Permite identificar particularmente un usuario o un sistema con un identificador único y diferenciarlo de otros.

**Autenticación**

Permite validar que el usuario o sistema que intenta acceder a un recurso es quien dice ser, mediante la validación de un mecanismo, por ejemplo, contraseña, pin, *token* o cualquier otro mecanismo asociado.

**Autorización**

Consiste en el permiso específico sobre el recurso al cual desea acceder, por ejemplo, un rol en una tabla de una base de datos.

**Importante**

Como factor fundamental de este control se debe considerar contar con mecanismos de auditoría que registren y/o alerten sobre accesos no permitidos, no autorizados o fallidos.

* 1. **Tipos de control para gestión de accesos**

El control para la gestión de los accesos puede ser abordado desde diferentes frentes de gestión o con distintas técnicas de control. La aplicación de dichos controles de gestión de accesos es un factor de garantía de la seguridad de la información en la organización; pero no solo de esta sino, además, de los activos de información, las personas, la infraestructura, entre otros.



<https://cdn.pixabay.com/photo/2018/07/05/12/47/gdpr-3518253_960_720.jpg>

Identifique, a continuación, algunos de las más comunes y funcionales controles:

CF6\_1-2\_Tipos\_De\_Control\_Gestion\_Accesos\_formato\_6\_slide\_diapositivas\_simple\_DI\_2023



* 1. **Características**

La implementación de los controles para la **gestión del acceso** debe contemplar ciertas condiciones que eleven la complejidad y dificulten el acceso no autorizado a los activos de información de la organización.



<https://media.istockphoto.com/photos/touch-screen-fingerprint-scanner-biometric-identity-of-a-womans-hand-picture-id1227405990?s=612x612>

Algunos ejemplos, se presentan a continuación:

**Privilegio mínimo**

Toda autorización de acceso debe darse de acuerdo con las necesidades de cada rol, por ejemplo, no hacer uso de credenciales de DBA en un usuario de conexión a través de una página web.

**Usuarios por defecto**

Reducir el uso de usuarios que vienen por defecto en los sistemas operativos o aplicaciones, ya que estos son utilizados en ataques de fuerza bruta.

**Actualización de credenciales**

Establecer los controles que requieran la actualización de contraseñas periódicamente.

**Uso de credenciales complejas**

Promover a través de controles el uso de contraseñas seguras.

**Almacenamiento de credenciales seguro**

Toda la información relacionada con información de usuarios debe almacenarse de manera segura, haciendo uso de algoritmos de cifrado unidireccional y bajo, con algún mecanismo de cifrado de base de datos.

1. ***Firewalls***

Son “un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad” (CISCO, 2021).



<https://cdn.pixabay.com/photo/2019/09/28/15/52/cyber-4511128_960_720.jpg>



Explore el siguiente video, en el cual se presenta una amplia explicación sobre los ***firewalls***, sus funcionalidades, tipos, características y otras generalidades que enriquecerán su conocimiento y formación.

¡**Adelante**!

CF6\_2\_FireWall\_​formato\_4\_video

1. **Sistemas de detección y prevención de intrusos IDS/IPS**

Existe otro tipo de soluciones que complementan la seguridad perimetral de una organización, a partir del análisis del tráfico de la red e identificando accesos no autorizados hacia algún recurso del perímetro. Los **IDS** (**Intrusion Detection System)**, *en español* Sistemas de detección de intrusión, son otro tipo de soluciones para el monitoreo de la seguridad perimetral, usada para detectar accesos no autorizados a un equipo o red.



<https://cdn.pixabay.com/photo/2019/07/16/11/42/vpn-4341631_960_720.jpg>

Se presentan algunos aspectos generales y de suma importancia relacionados con los sistemas de detección y prevención de intrusión IDS / IPS. Estúdielos con atención y lleve un registro en su libreta personal de apuntes.

CF6\_3\_Sistemas\_Prevencion\_y\_Deteccion\_Intrusos\_formato\_10\_tabs\_horizontales\_DI\_2023​



* 1. **Características funcionales de los IDS**

Tanto los IDS como los IPS cuentan con una serie de características que permiten no solo identificarlos, sino que además, dan la opción de reconocer tareas y funcionalidades que cumplen.



<https://cdn.pixabay.com/photo/2019/01/05/10/00/personal-data-3914809_960_720.jpg>

Dentro de las características más relevantes de los IDS se pueden enunciar las siguientes:

* Realiza el análisis del tráfico a partir de la verificación y comparación de patrones contra bases de datos con firmas conocidas de ataques maliciosos.
* Realiza el monitoreo permanente del tráfico que pasa por la red.
* Monitorea el comportamiento de los sistemas de información para identificar la intención de algún ataque.
* Identifica cambios en las configuraciones de los dispositivos o servicios.
* Emite alertas en gran variedad de sistemas.
* Requiere la actualización permanente de bases de datos con firmas actualizadas.
  1. **Características de los IPS**

Tanto los IDS como los IPS trabajan de manera conjunta, conformando una **segunda línea** **de seguridad** perimetral, complementando así las acciones y funciones de un *firewall*.



<https://cdn.pixabay.com/photo/2019/03/03/14/38/hacker-4031973_960_720.jpg>

Dentro de las características más relevantes de los OPS se presentan las siguientes:

* Complementa a los IDS, identificando y bloqueando conexiones con tráfico sospechoso.
* Permite descartar paquetes sospechosos.
* Permite bloquear direcciones sospechosas.

1. **Gestión unificada de amenazas UTM/XTM**

En el reconocimiento de soluciones para la gestión de la seguridad en organizaciones hay que mencionar un tipo de producto que ha venido abarcando un amplio campo, por el hecho de integrar en un solo dispositivo soluciones como las vistas hasta ahora en este componente (*firewalls*, IDS, IPS).



<https://cdn.pixabay.com/photo/2017/05/17/14/03/ransomware-2320941_960_720.jpg>

Se trata del **UTM** (Unified Threat Management) o Gestión unificada de amenazas. Con ellos están los **XTM** (Extensible UTM) o UTM Extendido, los cuales cubren las necesidades básicas más comunes, requeridas por las organizaciones en una única solución.

Se presentan los aspectos generales más importantes y definitorios de estos productos (**UTM/XTM**):

CF6\_4\_Gestion\_Unificada\_de\_Amenazas\_​

formato\_6\_slide\_diapositivas\_simple\_DI-2023

1. ***Antimalware***

En la actualidad es muy común escuchar del término ***malware***, pero puede no haber una definición clara del mismo; así como tampoco hay claridades unificadas sobre cómo combatirlo y evitar pérdidas o daños en los activos de información.



<https://cdn.pixabay.com/photo/2014/03/25/16/57/malware-297722_960_720.png>

El malware es un término amplio que describe cualquier programa o código malicioso, dañino para los sistemas. Puede invadir sistemas de información intrusivamente, causando daños, pérdidas de información, si no se está preparado.

Existen varios tipos de malware y tienen un impacto diferente, dependiendo de su funcionamiento:

* *Ransomware*.
* *Spyware.*
* *Adware.*
* Gusanos.
* Troyanos.
* *Robots*.

Un dispositivo afectado por malware puede presentar síntomas que anuncian dicha situación de afección por programas maliciosos:

* Lentitud del dispositivo.
* Falta de espacio en el disco sin causa alguna.
* Ejecución automática de programas o mensajes emergentes.
* Consumo excesivo de recursos (CPU, memoria RAM, tráfico de red, entre otros) sin razón alguna.
* Otros comportamientos relacionados.

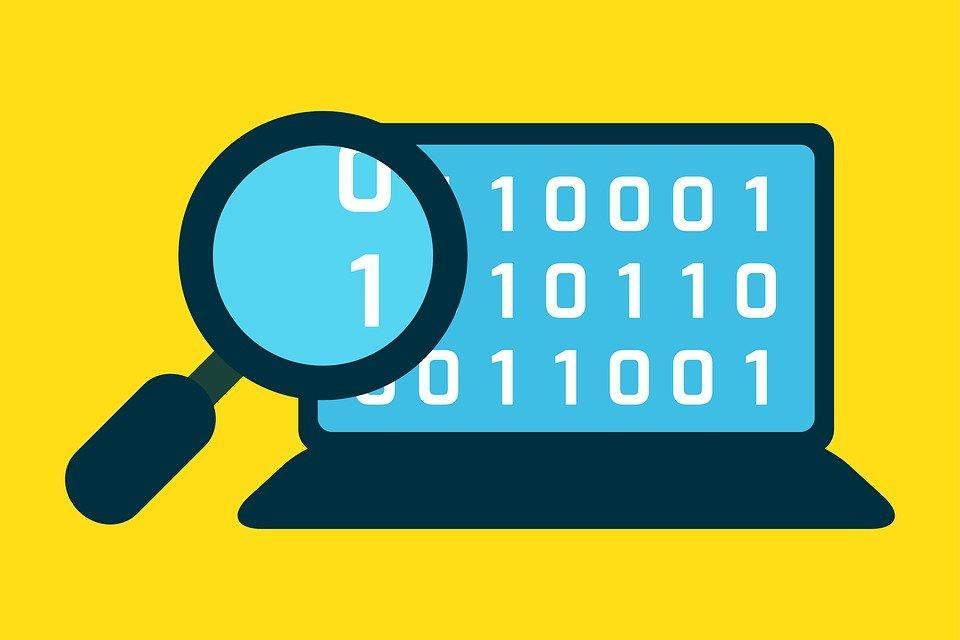
Como mecanismos de protección y para no sufrir afectaciones por este tipo de programas se recomienda el uso de tecnologías antimalware, que en la actualidad vienen integradas a las soluciones de antivirus como Norton 360, Avast, Mcafee, Kaspersky. También es posible encontrar soluciones independientes como Malwarebytes.

Las soluciones *antimalware* deben de incorporar características importantes como:

CF6\_5\_Soluciones\_antimalware\_formato\_9\_acordeon\_DI\_2023

1. **Detección y respuesta para *endpoints* (EDR)**

En ciertas ocasiones las soluciones no son suficientes para garantizar la seguridad de los activos de información de la organización; a pesar de todos los controles centralizados implementados aún existe un factor que puede ser el más vulnerable y es el factor humano.



<https://cdn.pixabay.com/photo/2020/02/07/21/33/data-4828441_960_720.jpg>

Pero ¿cuál o cuáles podrían ser las medidas apropiadas para superar la inseguridad digital causada por el personal de la organización? Revise una solución:

**Personal vulnerable**

El talento humano puede, de cierto modo, ser la puerta de entrada de los diferentes incidentes que pueden presentarse en la organización.

**Soluciones adicionales**

Es justo allí donde se propone otro tipo de soluciones que permiten mejorar la seguridad de los dispositivos de una red.

**Monitoreo de cambios en dispositivos**

Se trata de los EDR (**Endpoint Detection and Response**), en español Detección y Respuesta de *Endpoints,* los cuales permiten monitorear permanentemente los cambios presentados en los dispositivos.

* 1. **Aspectos clave de los EDR**

Un ***EndPoint*** puede ser cualquier dispositivo que se encuentra conectado a la red informática de la organización, por ejemplo, computadores, portátiles, teléfonos, servidores, *tablet*, etc. La detección y respuesta de EndPoints son aquellas soluciones que permiten detectar y responder ante actividades sospechosas en un dispositivo, de acuerdo con su comportamiento, evitando su reproducción o réplica en otros dispositivos de la organización.



<https://cdn.pixabay.com/photo/2015/01/08/18/24/programming-593312_960_720.jpg>

Las **EPP** (**Endpoint Protection Platform**), aquellas plataformas de protección *Endpoint*, son las soluciones integradas de seguridad que, por lo general, están conformadas por antivirus y *antimalware,* entre otros, y que operan comparando archivos con bases, si su firma corresponde.



* 1. **Tipos de soluciones de seguridad para *EndPoint***

Las soluciones de seguridad *Endpoint* permiten mantener bajo permanente monitoreo y control los dispositivos administrados; lo cual favorece realizar acciones a partir de políticas establecidas por el administrador de seguridad. Dependiendo del tipo de *Endpoint*, estos pueden presentar alertas, reportar a consolas centrales e incluso, aislar un dispositivo de la red cuando se presente una advertencia catalogada como crítica.



<https://cdn.pixabay.com/photo/2018/01/16/10/36/mistake-3085712_960_720.jpg>

Entre las soluciones para la gestión de la seguridad de los *Endpoint* existen los siguientes tipos de solución:

CF6\_6-2\_Tipos\_Soluciones\_Seguridad\_EndPoint\_formato\_10\_tabs\_verticales(pasos\_DI\_2023

* 1. **Características de las soluciones de seguridad**

Dentro de las características requeridas por una solución para la detección y respuesta de *Endpoints* es importante tener presente que deben abordarse los niveles de seguridad para este tipo de dispositivos.



<https://cdn.pixabay.com/photo/2016/12/18/03/25/cyber-security-1914950_960_720.jpg>

Acontinuación, se muestranlos niveles de seguridad para estos dispositivos. Haga la asimilación de ellos y procure llevar registro en su libreta personal de apuntes:

CF6\_6-3\_Caracteristicas\_Soluciones\_de\_Seguridad\_formato\_10\_tabs\_horizontales\_DI\_2023

1. **Cifrado**

Los controles de cifrado de información se han convertido en un elemento de gran importancia para la gestión de la seguridad de la información, ya que permite proteger la privacidad de la misma al evitar que esta sea interpretada por personas no autorizadas.

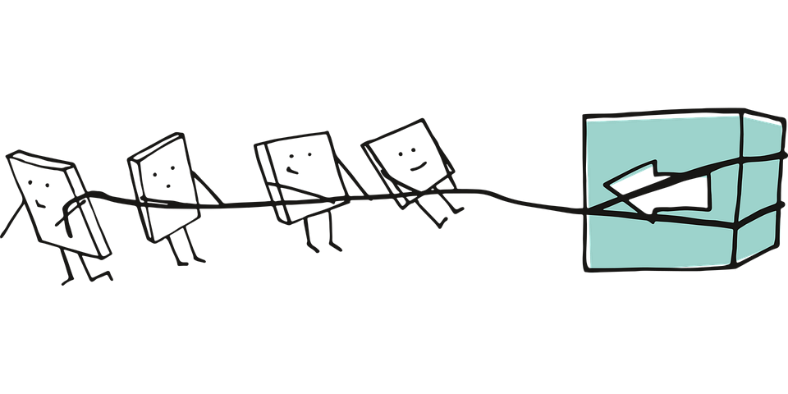


<https://cdn.pixabay.com/photo/2013/07/13/10/05/encrypted-156514_960_720.png>

Para profundizar en los aspectos conceptuales, operativos y funcionales del “**cifrado**”, correspondiente a este componente formativo, estudie atentamente el contenido del **Anexo\_1\_Cifrado**.

1. **Fuga de información**

La pérdida de información en una organización puede presentarse por varios factores. Esta pérdida y otros riesgos, sea en el nivel que sea, pueden ser mitigados y según la eficiencia en la aplicación de los controles y soluciones, podrían llegar a tener una mínima posibilidad de ocurrencia.



<https://cdn.pixabay.com/photo/2019/01/22/10/58/pixel-cells-3947910_960_720.png>

Preste mucha atención a las generalidades que, a continuación, se muestran sobre la **fuga de información en las organizaciones**:

CF6\_8\_Fuga\_de\_Informacion\_​

formato\_12\_rutas\_DI\_2023

* 1. **Prevención**

Que la organización conozca sus activos de información se considera el primer paso para tomar decisiones y acciones que prevengan incidentes relacionados con la fuga o pérdida de información.



<https://cdn.pixabay.com/photo/2018/02/13/06/59/smartphone-3149992_960_720.jpg>

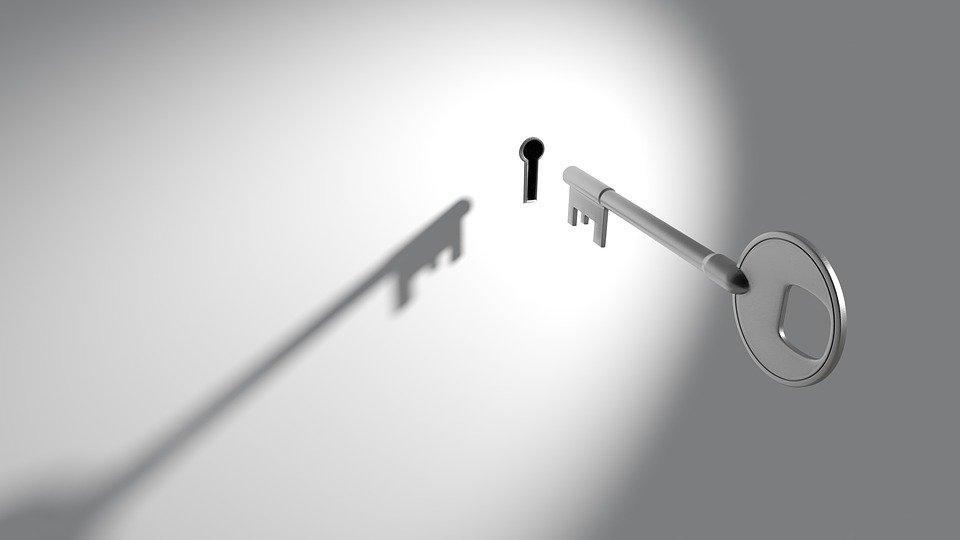
Para un proceso de conocimiento de activos pertinente se hacen las siguientes recomendaciones:

* Identificar los activos de la información que gestiona.
* Clasificar los activos de la información de acuerdo con su criticidad e importancia para la organización.
* Identificar el grado de seguridad actual, es decir, identificar los riesgos a los que está expuesto el activo de información.
* Implementar los controles que permitan mejorar la seguridad del activo de información.



* 1. **Recomendaciones para las organizaciones**

A las organizaciones en el marco del tratamiento de los riesgos por fuga o pérdida de información, y con mayor razón si se trata de organizaciones grandes o con gran nivel de administración de información se les recomienda el manejo de sistemas de prevención de pérdida de datos o DLP, así como la aplicación de controles orientados a la gestión del ciclo de vida de la información o ILM (*Information* *Lifecycle* *Management*).



<https://cdn.pixabay.com/photo/2017/03/03/13/56/key-2114046_960_720.jpg>

Estas son algunas recomendaciones adicionales para las organizaciones, referent4e al tratamiento y control de la fuga o robo de información:

**De dispositivos**

Desde luego, toda organización ha de adoptar herramientas de control de los dispositivos externos de almacenamiento, removibles y en línea, para evitar fugas de información.

**Organizativas**

Estos controles se relacionan con «la forma» en que se maneja o se trata la información. Por lo que se recomienda prevenir malas prácticas como compartir contraseñas o activos confidenciales, o hacer uso de contraseñas que son de conocimiento general. Esto conlleva a que se cuente con políticas de seguridad apoyadas en acciones de concienciación a todo el personal.

**Jurídicas**

Todos los empleados y proveedores deben cumplir con las políticas de seguridad; las cuales, en el caso de proveedores, se deben comunicar y aceptar mediante la firma de acuerdos de confidencialidad y de nivel de servicio (SLA)..

1. **Dispositivos móviles**

Dentro de la Norma ISO 27001 - Anexo A, se establecen los lineamientos de controles para el uso de dispositivos móviles, en función de las consideraciones de seguridad. En este punto del componente formativo podrá ahondar en aspectos y elementos de suma importancia en lo referente a **seguridad de la información y los dispositivos móviles**.

Para contextualizar sobre la seguridad de dispositivos móviles es importante tener presente los siguientes términos:

**Terminal**

Se conoce a cualquier dispositivo móvil que permite registrar y consultar información.

***Smartphone***

Teléfono inteligente que cuenta con funciones avanzadas para utilizar aplicaciones y gestionar información, estos dispositivos están compuestos por un sistema operativo, aplicaciones e información.

***Byod* (*Bring Your Own Device*)**

Es una tendencia por la cual optan algunas organizaciones, permitiendo que sus trabajadores utilicen sus dispositivos personales para el desarrollo de actividades laborales.

**Política de seguridad**

Son controles lógicos que se aplican a dispositivos, con el objetivo de controlar acciones o capacidades de un dispositivo móvil.

* 1. **Riesgos asociados**

Son muchas las amenazas de seguridad de información que en la actualidad podrían afectar negativamente los activos de información en las organizaciones y a las cuales están expuestas, especialmente, por el uso de dispositivos móviles sin control. El uso generalizado de los mismos y la necesidad de conexión a distintas redes de información favorecen esta situación.



<https://cdn.pixabay.com/photo/2016/12/14/09/40/facebook-1905890_960_720.jpg>

Entre los riesgos y amenazas más comunes y recurrentes se encuentran:

CF6\_9-1\_Riesgos\_Asociados\_Formato\_9-acordeon\_DI\_2023



* 1. **Controles**

De acuerdo con el control 6.2.1 de la Norma ISO 27001 Anexo A, se deben de establecer políticas que establezcan las medidas para la seguridad de la información gestionada a través de dispositivos móviles, y adoptar los controles necesarios para su administración.



<https://cdn.pixabay.com/photo/2012/04/13/20/24/laptop-33521_960_720.png>

Por ejemplo, se han de aplicar controles para configurar dispositivos móviles, procurando contar con un nivel básico de seguridad en los mismos.

1. **GuíaNIST-SP800-114**

Los procesos de ciberseguridad y seguridad de la información cuentan con orientaciones de las políticas internas de las organizaciones, las leyes vigentes de cada país, diferentes a las normas técnicas internacionales y guías.



<https://news.cyberwag.com/wp-content/uploads/2020/04/homeoffice.jpg>

Por su parte, el Instituto NIST ofrece la guía NIST-SP800-114 para el aseguramiento de actividades realizadas bajo la modalidad de teletrabajo y la adopción de la filosofía **BYOD** para el desarrollo de las actividades contractuales.

* 1. **Aspectos importantes de la guía**

La guía se encuentra estructurada por secciones que abordan los conceptos y las recomendaciones para la implantación de controles.



<https://www.iso27000.es/assets/images/nist-logo-225x225.png>

Las secciones destacadas de la guía y que ofrecen orientaciones fundamentales para los procesos de seguridad son:

* **La sección 2**: proporciona una descripción general del teletrabajo, el acceso remoto y una introducción a los problemas de seguridad relacionados con los dispositivos de teletrabajo.
* **La sección 3** proporciona pautas sobre cómo proteger la información almacenada o enviada desde o hacia dispositivos de teletrabajo.
* **La sección 4** presenta recomendaciones para proteger las redes domésticas alámbricas e inalámbricas que se utilizan para el teletrabajo.
* **La sección 5** trata sobre la protección de las computadoras personales (PC) BYOD, a través de métodos como la aplicación de actualizaciones de *software*, la instalación y configuración de *software* antivirus y *firewalls* personales.
* **La sección 6** ofrece una descripción general de la protección de dispositivos móviles BYOD.

****

* 1. **Seguridad en el teletrabajo**

Las organizaciones actualmente vienen habilitando las posibilidades para que su personal pueda desarrollar sus actividades sin que necesariamente se encuentren en la sede física, atendiendo, además, la reglamentación legal y laboral, estas deben garantizar que los empleados cuenten con los recursos necesarios para el desarrollo de sus actividades, entre estas se encuentran las condiciones de seguridad.



<https://cdn.pixabay.com/photo/2019/05/10/19/45/office-4194326_960_720.jpg>

Por lo anterior, se sugiere considerar las siguientes recomendaciones adicionales para el desarrollo de actividades bajo la modalidad de teletrabajo.

* Uso de equipos adecuados.
* Garantizar el acceso a la información, de acuerdo con las condiciones y controles de seguridad anteriormente nombrados.
* Contar con mecanismos de conexión segura, evitando hacer uso de canales abiertos y públicos.
* Proveer de herramientas actualizadas contra *malware*.
* Mantener un monitoreo permanente del tráfico de la red donde se encuentran los activos de información.
* Contar con políticas de seguridad implementadas e informadas a todo el personal.

1. **Infraestructuras críticas**

Es momento de abordar algunos conceptos importantes en el aseguramiento de infraestructuras críticas, aquellas que se han convertido en industrias de orden principal en el país. Se trata de aquellas “infraestructuras estratégicas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales” (LISA Institute, 2020).



<https://www.lanner-america.com/wp-content/uploads/Critical-INfrastructure-Protection-Challenges-2018-1.jpg>



Las infraestructuras críticas abordan sectores primordiales para el desarrollo de las regiones. En la siguiente herramienta visualice los diferentes ámbitos de las mismas y profundice en sus aspectos clave:

CF6\_11\_Infraestructuras\_criticas\_formato\_2\_infografia\_interactiva\_puntocaliente\_DI\_2023

1. **Mejoras de ciberseguridad en infraestructuras**

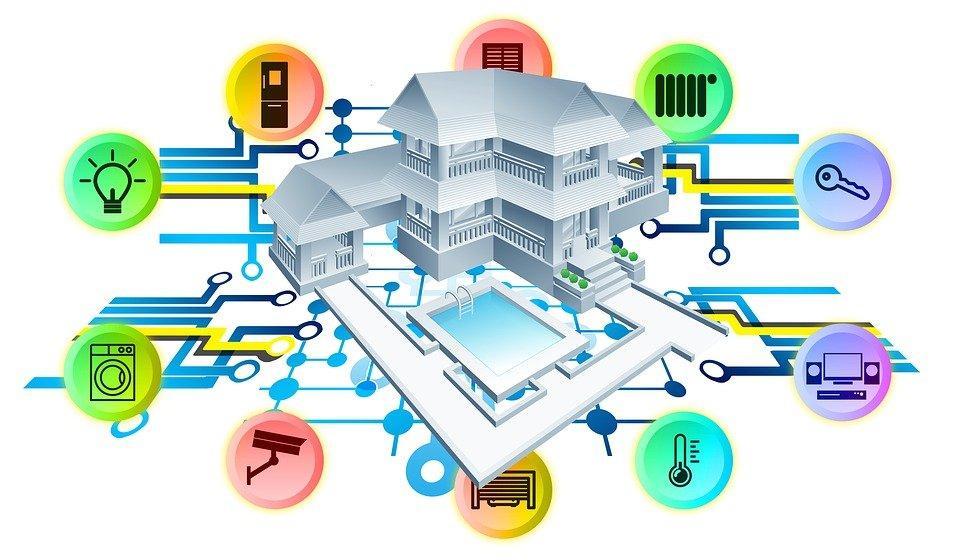
Para la gestión de las infraestructuras críticas, dada su complejidad, es importante contar con un marco que le permita realizar una mejora continua a su nivel de seguridad. El NIST (*National Institute of Standards and Technology*) en el año 2018 publicó el *Framework for Improving Critical Infrastructure Cybersecurity*, con el cual busca promover una adecuada gestión de los riesgos de la ciberseguridad en las organizaciones, adoptando las mejores prácticas de ISO, ITU, CIS, NIST, entre otros.

Estudie en detalle el **Anexo\_2\_MejorasDeCiberseguridadEnInfraestructuras** y profundice en los aspectos más importantes en el proceso de gestión de los riesgos de la ciberseguridad en las organizaciones.

1. **Sistemas de correlacionamiento de *logs* y monitoreo**

Los sistemas para el correlacionamiento de *logs* y monitoreo de la actividad que pasa sobre las redes y dispositivos permiten una visión actualizada del nivel de seguridad de los controles implementados. Mantener una vista del estado de la seguridad de una red requiere de herramientas que permitan representar fácilmente la información consolidada.

Tal información de monitoreo proviene de los activos de información y de los controles implementados, los cuales son los encargados de reportar las acciones realizadas.



<https://cdn.pixabay.com/photo/2017/09/20/16/59/smart-home-2769239_960_720.jpg>

Estos son algunos conceptos y datos clave a tener en cuenta:

**Correlacionados de eventos / SIEM**

Estas soluciones especializadas brindan la capacidad de crear centros de monitoreo a partir de las fuentes de información recolectadas como, por ejemplo, registro de un servidor web, registros de auditoría de un servicio LDAP, etc.

**Sensor**

Mecanismos encargados de monitorear el comportamiento de un servicio o de un dispositivo, permitiendo recolectar la información sobre algún comportamiento irregular, por ejemplo, un sensor para monitoreo de servicio web.

**IDS / IPS**

Estos sensores pueden ser IDS, IPS, sistemas de monitoreo, como, por ejemplo, Snort, Suricata, etc.

**Dashboard**

También llamados tablero de control, es una herramienta visual que representa mediante gráficas el estado actual de la red o puede presentar las alertas a las que se debe prestar atención.

**Registro *log***

Es un historial de registros de eventos ordenados en orden cronológico y almacenan la información de diferentes eventos como, por ejemplo, del sistema operativo, servicio o registro de autenticación desde una aplicación.



1. **Gestión de eventos e información de seguridad SIEM**

Un **SIEM** es “una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager)” (INCIBE, 2020), como se muestra en la siguiente figura:

**Figura 1**

*Funcionalidades de un SIEM*

****

<https://v-valley-mcafee.es/uploads/noticias/flujo_siem.JPG>

Descubra a continuación, los aspectos más importantes sobre la gestión de eventos de información de seguridad SIEM, sus esquemas lógicos, proveedores, entre otros.

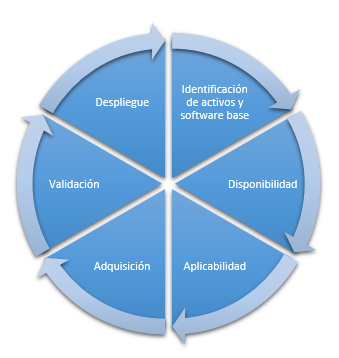
CF6\_14\_Gestion\_Eventos\_Informacion\_SIEM\_formato\_10\_tabs\_horizontales\_DI\_2023

1. **Parcheado y/o actualización**

La gestión de las actualizaciones y parcheo de los sistemas de información o de los dispositivos de la organización se convierten en un factor fundamental para garantizar la seguridad de la información, ya que a partir de esta gestión se puede reducir amenazas por desactualización de sistemas y evitar que terceros puedan aprovecharla, como se muestra en la siguiente figura:

**Figura 2**

*Fases para la gestión de parches y/o actualizaciones*



<https://www.incibe-cert.es/sites/default/files/blog/parches_industria/proceso.png>

Los parches o actualizaciones son cambios que se aplican a los sistemas de información, sistemas operativos o incluso dispositivos *hardware* con los cuales se busca corregir errores, vulnerabilidades o implementar mejoras de los sistemas.

Para realizar una adecuada gestión de parches y/o actualizaciones se recomienda seguir metodologías apoyadas en soluciones que faciliten este trabajo. Tenga presentes las fases que se enuncian a continuación:

* **Identificación de activos y *software* base**: mantener un inventario actualizado de los detalles de los activos de información, con el fin de determinar las actualizaciones correspondientes.
* **Disponibilidad**: identificar cuál parche específico, requerimientos y orden correspondiente debe aplicarse a cada uno de los sistemas y así evitar daños en sistemas por incompatibilidades.
* **Aplicabilidad**: verificar si la actualización es aplicable a cada sistema de información, ya que no siempre los parches son compatibles con todos los dispositivos.
* **Adquisición**: se recomienda que los archivos para la actualización o parcheo sean adquiridos a través de medios o fuentes confiables, preferiblemente de las casas productoras.
* **Validación**: se recomienda siempre realizar una validación previa y posterior a la actualización, con el fin de prevenir la pérdida de información o el no funcionamiento de dichos sistemas.
* **Despliegue**: realizar la programación de despliegue, incorporando los archivos necesarios y documentación sobre el proceso de implementación, así como la resolución de problemas más comunes.

** **

**Síntesis**

La aplicación de estrategias de ciberseguridad implica el uso de medidas y

procedimientos para proteger sistemas, redes y datos contra amenazas cibernéticas,

como ataques de hackers, malware y brechas de seguridad. Estas estrategias incluyen

políticas, tecnologías y prácticas para prevenir, detectar y responder a amenazas

cibernéticas, asegurando así la integridad, confidencialidad y disponibilidad de la

información digital.

**Diagrama

Descripción generada automáticamente**

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

|  |  |
| --- | --- |
| Descripción de la actividad didáctica | |
| Nombre de la actividad | RELACIONAR TÉRMINOS |
| Objetivo de la actividad | Identificar conceptos para aplicación de estrategias de ciberseguridad conforme a la planificación realizada |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | CF6\_228124\_DI\_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 |
| Dispositivos móviles | Organización Internacional de Normalización. (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad*. ISO 27001. <https://www.iso.org/standard/54534.html> | Norma técnica | <https://www.iso.org/standard/54534.html> |
| 1. Guía NIST-SP800-114 | NIST. (2021). *Cybersecurity framework*. NIST. <https://www.nist.gov/cyberframework> | Página web | <https://www.nist.gov/cyberframework> |

1. **Glosario**

|  |  |
| --- | --- |
| Término | Significado |
| Auditoría: | proceso mediante el cual se busca verificar o validar que se esté cumpliendo una condición o la aplicación de un control. |
| Control: | mecanismo de tipo lógico o técnico con el cual se busca regular o establecer restricciones de alguna acción. |
| *Framework*: | es un marco de trabajo que provee los componentes y condiciones necesarias para su aplicación. |
| Intrusión: | acceso no autorizado a un sistema o activo de información sin consentimiento del propietario. |
| Log: | registro secuencial sobre eventos presentados en un sistema de información. |
| *Malware*: | programa dañino que se instala en dispositivos y que puede generar daños o pérdida de información. |
| Riesgo: | es la probabilidad de que una amenaza se materialice generando alguna consecuencia negativa. |

1. **Referencias bibliográficas**

Audea. (2010). *Fuga de información ¿Qué es y cómo se puede prevenir?* Audea. <https://www.audea.com/fuga-de-informacion-que-es-y-como-se-puede-prevenir/>

Cisco. (2021). *¿Qué es un firewall?* Cisco. <https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html>

FORTINET. (2021). *Administración unificada de amenazas.* FORTINET. <https://www.fortinet.com/lat/products/smallbusiness/utm>

Instituto Nacional de Ciberseguridad. (2017). *Control de acceso. Políticas de seguridad para la pyme.* Incibe*.*  <https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf>

Instituto Nacional de Ciberseguridad. (2020). *¿Qué son y para qué sirven los SIEM, IDS e IPS?* Incibe. <https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips>

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

LISA Institute. (2019). *¿Qué son las infraestructuras críticas?* LISA Institute. <https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas>

Malwarebytes (2021). *Todo acerca del* *malware*. Malwarebytes. <https://es.malwarebytes.com/malware/#what-is-malware>

NIST. (2021). *Marco de ciberseguridad.* NIST.<https://www.nist.gov/cyberframework>

SeguriLatam. (2020). *Seguridad en dispositivos móviles: ¿cuáles son las ciberamenazas más peligrosas?* SeguriLatam. <https://www.segurilatam.com/actualidad/ciberseguridad-seguridad-en-dispositivos-moviles-cuales-son-las-ciberamenazas-mas-peligrosas_20201005.html>

Server World. (2020). *Apache2: configure SSL/TLS.* Server World. <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=httpd&f=3>

Welivesecurity. (2021). *Todo sobre cifrado: qué es y cuándo deberías usarlo*. Welivesecurity. <https://www.welivesecurity.com/la-es/2016/02/09/todo-sobre-cifrado-cuando-usarlo/>

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 | Septiembre 2021 |
| Carolina Coca Salazar | Revisora metodológica y pedagógica | Regional Distrito Capital- Centro de Diseño y Metrología | Septiembre 2021 |
| Julia Isabel Roberto | Diseñadora y evaluadora instruccional | Regional Distrito Capital- Centro para la Industria de la Comunicación Gráfica | Septiembre 2021 |

1. **Control de cambios**

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| Autor (es) | Nelly Parra Guarín | Adecuadora Instruccional | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
|  | Alix Cecilia Chinchilla Rueda | Asesora Metodológica | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
|  | Liliana Victoria Morales Guadrón | Responsable Línea de Producción Distrito Capital. | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |