Guion para desarrollo de contenidos

**Datos de identificación del programa de formación**

| PROGRAMA DE FORMACIÓN | Técnico en control de la seguridad digital |
| --- | --- |

| COMPETENCIA | 220501111. Controlar sistema de seguridad de la información de acuerdo con los procedimientos y su normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-03. Operar herramientas de control de la seguridad digital para mitigar los riesgos según procedimientos técnicos de la política de seguridad digital. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 7 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Ciberseguridad, herramientas de monitoreo y control |
| BREVE DESCRIPCIÓN | En este material se introduce al aprendiz en la configuración, operación, validación y verificación de herramientas de control de seguridad digital, que permiten mitigar los riesgos según procedimientos técnicos de la política y normatividad de la ciberseguridad, aspecto fundamental para verificar la funcionalidad y el cumplimiento de la cadena de custodia de los incidentes.(54) |
| PALABRAS CLAVE | Control de activos, copia de seguridad, informes, sistemas de gestión. |

| ÁREA OCUPACIONAL | 1 – FINANZAS Y ADMINISTRACIÓN |
| --- | --- |
| IDIOMA | Español |

# TABLA DE CONTENIDOS

**Introducción**

**1. Gestión de hardware y software**

1.1. Manuales técnicos

1.2. Configuración básica de equipos

**2. Monitoreo de equipos**

2.1. Herramientas de monitoreo y gestión

2.2. Herramientas de protección y control

**3. Respuesta a incidentes**

3.1. Validación de controles de seguridad

3.2. Cadenas de custodia

**Síntesis**

**INTRODUCCIÓN**

| Cuadro de texto |
| --- |
| En este recurso educativo se describen las herramientas para el control de incidentes en ciberseguridad, sin que se profundice en el impacto de estos. De este modo, el enfoque se centrará principalmente en la parametrización de *hardware* y *software*, seguridad en sistemas operativos, mecanismos como la criptografía, seguridad perimetral y plataformas de auditorías. Por último, se revisará de forma general la detección de incidentes de seguridad.  Lo mencionado es necesario para implementar y controlar las prácticas de seguridad digital en las organizaciones con apoyo de herramientas que logren minimizar los efectos de los incidentes. Las instituciones en la actualidad están expuestas a vulnerabilidades que pueden ocasionar pérdida de información, daños en equipos de la red o suplantación, lo cual puede generar desconfianza, mal funcionamiento o cierre de la entidad. No se puede asegurar que existe una empresa en el mundo con todos sus procesos completamente protegidos.  Para iniciar, por favor ver el video introductorio en el que se hace una reseña general de cada uno de los temas a desarrollar en este componente formativo. ¡Muchos éxitos en esta aventura de aprendizaje! |

**GUION DE VIDEO INTRODUCTORIO**

| **Tipo de recurso** | Video spot animado | | | |
| --- | --- | --- | --- | --- |
| **NOTA** | **La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente** | | | |
| **Título** | Herramientas de monitoreo y control | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración (voz en off)** | **Texto** |
| **1** | Un carrusel de imágenes de equipos de computadores con virus o con alertas de peligro de robo de información, alternando con el texto.  hacker de computadora con teléfono - robo de información fotografías e imágenes de stock  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ladrón. hackers roban la carpeta de documentos de datos confidenciales de computadora útil para anti phishing y internet campañas de virus. concepto hacking red social en internet. - robo de información  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de estafa de phishing, seguridad web y ataque hacker vector concepto - robo de información | Puede ser música instrumental o la que considere que funciona perfecto para el tema y las animaciones que se realicen del video | Con el acceso a la información a través de internet y la divulgación de archivos clasificados como secretos por medios masivos de comunicación, las personas se han enterado de los delitos cibernéticos y robos de información a grandes empresas denominadas ‘gigantes del internet’.  Por ejemplo, en el año 2019, piratas cibernéticos vulneraron los protocolos de seguridad y robaron más de 500 millones de datos de los usuarios de una de las redes sociales más importantes del momento, incluido el número de teléfono, ubicación e información personal de su fundador (Kaspersky, s.f.). | Delitos cibernéticos  Robos de información |
| **2** | Realizar una especie de historieta simulando el caso que se describe en la narración sobre el ataque cibernético. Imágenes de robo de información, virus, etc.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de phishing de datos, ataque de hackers. - robo de información  Ciberseguridad Seguridad tecnológica digital - Foto de stock de Medidas de seguridad libre de derechos  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de hacker - robo de información | Puedes ser música instrumental o la que consideren que funciona perfecto para el tema y las animaciones que realicen del video | Del mismo modo, para junio de 2020 un gigante de la industria automotriz se vio afectado por un ataque en sus oficinas de Estados Unidos, Europa y Japón. El efecto fue inmediato, la empresa frenó la producción en diversas regiones para tratar de mitigar los incidentes de su red. Los atacantes lograron ingresar en los servidores y encriptaron la información, para exigir el pago por el rescate, el cual, hasta el momento, es un misterio. | Un ataque cibernético puede llevar a parar el funcionamiento de una empresa  Genera gran des pérdidas económicas y de información |
| **3** | Animaciones de imágenes y texto. Personal de seguridad, antivirus…concepto de software antivirus - ntivirus fotografías e imágenes de stock  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de banner isométrico para protección de datos de internet - ntivirus  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de seguridad protección y cyber. - antivirus | Puede ser música instrumental o la que consideren que funciona perfecto para el tema y las animaciones que se realicen del video | En este sentido, la masificación del internet ayudó al crecimiento y escalabilidad de las compañías, permitiéndoles llegar a mercados que físicamente era imposible ocupar, pero también introdujo innumerables retos en cuanto a ciberseguridad, haciendo que tengan que invertir grandes cantidades de dinero en herramientas y personal capacitado. Las inversiones en estos rubros hoy en día, se pueden contar como un activo, y no como un gasto, debido a que la vulnerabilidad de los sistemas y las redes pueden ocasionar grandes daños económicos, como los casos expuestos anteriormente. | Inversión en ciberseguridad es un ‘activo’  Herramientas para el control y protección de información  Personal capacitado |
| **4** | Recrear un personaje y un carrusel de imágenes con cada texto en la que diferentes personas, a través, de un equipo o dispositivo realice labores de control de seguridad  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de hombre con una espada enorme junto a un teléfono inteligente. escudo con cerradura. protección de datos en aplicaciones móviles, internet, mensajeros. ciberseguridad online. ilustración plana vectorial. - antivirus    ilustraciones, imágenes clip art, dibujos animados e iconos de stock de empresario hacia fuera desde una computadora con un escudo - antivirus    trabajando para una experiencia de internet más sequre - antivirus fotografías e imágenes de stock    ilustraciones, imágenes clip art, dibujos animados e iconos de stock de conjunto de concepto de piratería isométrica. conjunto de ilustraciones de virus informáticos, protección contra la piratería, ataque de hackers. anti virus, spyware, malware. ilustración vectorial - antivirus | Puede ser música instrumental o la que consideren que funciona perfecto para el tema y las animaciones que se realicen del video | Como futuro técnico en el área de seguridad digital, es su deber conocer, configurar, operar, implementar, validar y verificar herramientas y controles para gestión de incidentes, con el fin de mitigar los riesgos e incidencias de los ciberataques. Toda la parte operativa de las herramientas se rige bajo estrictos ordenamientos o plataformas de auditorías, como, por ejemplo, las auditorías de *logs* que integra la guía nist sp 800-92, correlacionadores de eventos, revisión de patrones de ataque, metodologías, y revisión de archivos *logs.* De ellas, se puede resumir que se genera todo un proceso en la detección de incidentes de seguridad, que, a su vez, contempla subprocesos como: monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información, y la creación de copias de seguridad. | Gestionar los incidentes  Mitigar riesgos  Conocer y configurar plataformas de auditorías para realizar:  -Revisión de patrones de ataque  -Detección de incidentes  -Monitoreo y control  -Creación de copias de seguridad |
| **5** | Animación de imágenes y texto  Criptografía  criptomoneda en la aplicación de comercio binance, bitcoin btc con moneda digital altcoin criptomoneda, bnb, etereum, dogecoin, cardano, defi p2p descentralizado mercado fintech - criptomoneda fotografías e imágenes de stock    Algoritmos  programación de código fuente en pantalla digital. desarrollador de software y lenguaje html de programación de internet. concepto de diseño web php y css. metadatos y tecnología seo. - algoritmos fotografías e imágenes de stock    Firmas digitales  firma electrónica en pantalla de smartphone. - firmas digitales fotografías e imágenes de stock  Las llaves  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de página de inicio isométrica de protección de datos personales - seguridad digital  Los *tokens*  registro sobre el uso de un segundo factor modo de autenticación - tokens fotografías e imágenes de stock  Las *Smart Cards*  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de isométrico teléfono móvil y banca por internet. operación de seguridad de pago en línea mediante tarjeta de crédito. - smart cards  La biometría  mano de chino asiático con blazer puesto en la pantalla del dispositivo escáner para el acceso de control de seguridad - biometría fotografías e imágenes de stock  Las aplicaciones  concepto de protección de datos, ciberseguridad, acceso seguro con contraseña - aplicaciones de seguridad fotografías e imágenes de stock | Puede ser música instrumental o la que consideren que funciona perfecto para el tema y las animaciones que se realicen del video | Sin embargo, para que una auditoría resulte ser eficiente y logre consolidar toda la información, es necesario tener en cuenta los mecanismos de seguridad y su conceptualización, los cuales han venido avanzando a través del tiempo. Entre estos se destacan: la criptografía clásica y moderna, los algoritmos asimétricos, las firmas y los certificados digitales, las llaves, los *tokens*, las *smart cards*, la biometría. De igual forma, se incluyen las aplicaciones como kerberos, pgp, ssh, protocolos/ssl/tls//s-mime, PKI, IPSEC, y estenografía, sin dejar de lado los manuales técnicos y especificaciones del fabricante de *hardware* y *software*.  Así que, sin más preámbulo, se le da la bienvenida al estudio de este componente formativo.  ¡Anímese a explorar todos los recursos educativos! (505) | Mecanismos de seguridad  Criptografía clásica y moderna  Algoritmos asimétricos  Firmas y los certificados digitales  Las llaves  Los t*okens*  Las *smart cards*  La biometría  Las aplicaciones de seguridad |
| **Nombre del archivo** | **233103\_CF07\_v1.mp3** | | | |

**DESARROLLO DE CONTENIDO**

**1.** **Gestión de hardware y software**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| El Internet y la masificación del uso de las Tecnologías de la Información y las Comunicaciones (TIC) ha incrementado los usuarios digitales en todos los sectores de la economía; cada vez se puede observar personas de diferentes edades haciendo uso de los medios digitales para comprar o vender productos, adquirir servicios o, simplemente, realizar transacciones bancarias, lo que conlleva a que puedan estar expuestas a eventuales fraudes, suplantación de identidad o robos de información. | |

| **Tipo de recurso** | Slider Presentación | |
| --- | --- | --- |
| **Introducción** | Por lo anterior, es importante tener en cuenta las mejores prácticas o procedimientos de seguridad de la información o ciberseguridad, cómo los que se describen a continuación. | |
| Primero  Optar por *software* que pueda proteger las actividades que se realizan a través de los medios digitales. Es importante obtener estos programas de sitios oficiales o que cuenten con buena reputación, esto disminuye la eventualidad que al interior de las carpetas introduzcan algún tipo de *software* dañino que se apodere de la información del equipo desde el cual se está realizando las actividades. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de aplicación de pc y smartphone con gráfico de negocios y datos analíticos. ilustración vectorial isométrica del mecanismo de protección digital, privacidad del sistema. datos seguros. mercado monetario digital, inversión - software de seguridad  **Cod.Imagen:** 233103\_i1 |
| Segundo  Hacer uso de buenas prácticas descritas en la norma ISO 27000, por ejemplo, revisar constantemente la actividad del antivirus instalado en el equipo; confirmar que esté activo, con las bases de datos actualizada, y en lo posible activar la función de navegador seguro, debido a que se puede instalar una extensión del antivirus al navegador predeterminado y generar las alertas al tratar de acceder a un sitio no seguro. También, revisar la URL de la página a la cual se va a acceder, verificando que cuente con el certificado *Secure Sockets Layer* (SSL), este constituye una serie de protocolos criptográficos que suministra comunicaciones seguras a través de la red.  Para saber si la página cuenta con este, al lado de la URL aparece un ícono de un candado o la URL termina con una ‘s’ (https en lugar de http); además, en aquellos sitios que sugieren crear cuentas para poder acceder, es importante crear contraseñas seguras que sean difíciles de descifrar. Aquí puede encontrar algunas recomendaciones:   * Mínimo 8 caracteres alfanuméricos (a, b,1,4,7…) * Que contenga mínimo una letra en mayúscula (A, B, C, …Z). * Que contenga mínimo una letra en minúscula (a, b, c, z) * Que contenga mínimo un número (0,1, 2, 3…9). * Que contenga mínimo un carácter especial (¡°|#$%&/()=?¡\*+}{}[[.,-…). | | empresario sosteniendo tableta y mostrando la mejor garantía de calidad con cinco estrellas doradas para garantizar el producto y el concepto de servicio iso. - norma iso fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i2 |
| Tercero  Además del uso del *software* y buenas prácticas, es igual de importante la inversión en herramientas que permitan aumentar el nivel de seguridad. En este sentido, es posible hallar *hardware* cuyo precio y aplicaciones pueden variar; sin embargo, es importante recordar que en el tema de la seguridad no existen gastos innecesarios. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de centro de datos de nodal isométrico 3d con espacio de trabajo, diagrama y laptop. - herramientas de seguridad digital  **Cod.Imagen:** 233103\_i3 |

| Cuadro de texto |
| --- |
| Para implementar procedimientos asociados a la seguridad digital son necesarias algunas herramientas.  En el siguiente video se explican con detalle herramientas de *hardware* y *software*. |

| **Tipo de recurso** | Video animación 2D | | | |
| --- | --- | --- | --- | --- |
| **NOTA** | **La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente** | | | |
| **Título** | **Herramientas de Hardware y Software** | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración** | **Texto** |
| **1** | Recrear un personaje que narre y explique cada herramienta, según el texto y con muestra de imagen de la herramienta.  Llave U2F  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de token de seguridad con contraseña - token | Por favor un sonido acorde a las animaciones de texto e imágenes y narración | Querido aprendiz: en esta nota de video se describen algunas herramientas de *hardware* y *software* útiles para implementar sistemas de seguridad informática en las organizaciones.  Se iniciará con las herramientas tipo *hardware*, dentro de las que se encuentran las ‘llaves U2F’,que consisten en una unidad USB de doble autenticación que permite generar claves para ingreso seguro en diversos lugares. La persona que no posea esta llave, no podrá vulnerar las cuentas del propietario. | Llaves U2F  Token de seguridad con contraseña |
| **2** | Firewall por hardware  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ilustración plana personas que trabajan juntas para guardar big data en datos en la nube esta es una tecnología moderna que permite almacenar más datos sin tener que llevar un disco duro. - equipo firewall  Router VPN y VPN Box  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de conexión vpn seguro. resumen de la conectividad de red privada virtual. ilustración de vector. - router vpnestante del servidor moderno aislado sobre fondo blanco. - vpn box fotografías e imágenes de stock | Por favor un sonido acorde a las animaciones de texto e imágenes y narración | El ‘firewall por hardware’es una unidad física tipo *box* que protege la red de amenazas externas. El dispositivo se instala entre el servidor y el internet, permitiendo o denegando el acceso de datos.  Los ‘*router VPN’* y *‘VPN Box’* son dispositivos que soportan redes virtuales privadas (VPN) con el propósito de redirigir el tráfico de t a través de aquellas privadas seguras. | Firewall por hardware  Tecnología de almacenamiento de datos.  *Router VPN – VPN Box*  Redirige tráfico de internet. |
| **3** | El mismo personaje narrando y en coherencia que se visualicen las imágenes y el texto según la herramienta.  Hardaware de cifrado  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de aplicación de smartphone con gráfico de negocios y datos analíticos en teléfono móvil isométrico. tendencias de análisis y concepto de proceso de codificación de desarrollo de software. programación, prueba de código multiplataforma - hardware de cifrado  Token PKI  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de inicio de sesión único - sso - ilustración 3d - hardware de tokens | Por favor un sonido acorde a las animaciones de texto e imágenes y narración | El ‘*hardware* de cifrado’ es un procesador que maneja cifrado de los datos mediante clave pública o privada. Su función es alojar algoritmos que permiten cifrado o descifrado de esos datos.  Los ‘*tokens* PKI’o *Public Key Infrastructure* (infraestructura de clave pública) son un sistema que proporciona certificados digitales, además de claves privadas. | *Hardware* de cifrado  Cifrado de datos  Tokens PKI  Infraestructura de clave pública |
| **4** | El mismo personaje narrando y en coherencia que se visualicen las imágenes y el texto según la herramienta.  Acelerados SSL/TLS  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de procesamiento seguro de pagos en línea - hacer pagos seguros en línea - ilustración 3d - ssl  Sistema de pago seguro  pago sin contacto  - sistema de pago seguro fotografías e imágenes de stock | Por favor un sonido acorde a las animaciones de texto e imágenes y narración | El ‘acelerador SSL/TLS  *Secure Sockets Layer’* (SSL) son protocolos criptográficos que se utilizan con certificados de confianza para garantizar la comunicación segura.  El ‘sistema de pago seguro por *hardware’* permite el pago electrónico a través de tarjetas físicas, mediante datáfonos que pueden soportar banda magnética, chip, o tarjeta de proximidad. | Acelerador SSL/TLS  Procesamiento seguro de pagos en línea - Hacer pagos seguros en línea.  Sistema de pago seguro por *hardware*  Pago sin contacto. |
| **5** | El mismo personaje narrando y en coherencia que se visualicen las imágenes y el texto según la herramienta.  Cartera digital  concepto de pago mediante tarjeta de crédito. transacción de pago en línea segura con teléfono inteligente. banca por internet a través de tarjeta de crédito en el móvil. ilustración 3d - cartera digital fotografías e imágenes de stock  Sensores biométricos  mano de chino asiático con blazer puesto en la pantalla del dispositivo escáner para el acceso de control de seguridad - sensores biométricos fotografías e imágenes de stock  Candado Kensington  Amazon.com: Kensington ClickSafe K68105WW - Candado universal para portátil  : Electrónica | Por favor un sonido acorde a las animaciones de texto e imágenes y narración | La ‘cartera digital’ o también conocida como *e-wallet* es un espacio virtual donde se almacenan datos bancarios, tarjeta de crédito, entre otros.  Los ‘sensores biométricos’ son sistemas mecánicos o electrónicos que se usan para leer o capturar las huellas dactilares.  El ‘candado universal para portátiles’ es un seguro con cable de seguridad utilizado para anclar los laptop en un lugar fijo. | Cartera digital  Concepto de pago, banca por Internet a través de tarjeta.  Sensores biométricos  Escáner para el acceso de control de seguridad  Candado Kensington o similares  Candado universal para portátil |
| **6** | El mismo personaje narrando y en coherencia que se visualicen las imágenes y el texto según la herramienta.  Antivirus  delito cibernético. la inscripción en el antivirus del teclado, dedo presiona una tecla en el ordenador portátil. el concepto de éxito en línea. - antivirus fotografías e imágenes de stock    ilustraciones, imágenes clip art, dibujos animados e iconos de stock de protección de datos digitales - firewall | Por favor un sonido acorde a las animaciones de texto e imágenes y narración | Dentro de las herramientas de *software* se encuentran:  El ‘antivirus’, que consiste en un programa que ofrece protección efectiva cuando el equipo se encuentra expuesto a *software* malicioso o cualquier otro tipo de *malware.*  El ‘*firewall’* es un sistema para prevenir y proteger la red privada de ataques de otras redes. | Antivirus  Programa de protección contra s*oftware* malicioso  *Firewall*  Sistema de prevención de ataques |
| **7** | El mismo personaje narrando y en coherencia que se visualicen las imágenes y el texto según la herramienta.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ilustraciones vectoriales abstractas de concepto de transferencia de datos en línea. - proxy    protección de datos o red, empresarios presionan icono de escudo, seguridad antivirus. protección de datos y seguros conceptos de seguridad empresarial, seguridad de la información contra virus. número binario 1010. - servicio de seguridad informatica fotografías e imágenes de stock | Por favor, un sonido acorde a las animaciones de texto e imágenes y narración | El ‘*proxy*’ es un programa o dispositivo físico que actúa de intermediario entre conexiones del navegador e internet, filtrando todos los paquetes entre ambos.  El ‘MDR – *Managed Detection and Response’* es un servicio en seguridad avanzado, donde se proporciona la búsqueda de amenazas y el monitoreo inteligente. | *Proxy*  Programa intermediario para filtrar  MDR – *Managed Detection and Response*  Servicio de seguridad detección de amenazas |
| **8** | El mismo personaje narrando y en coherencia que se visualicen las imágenes y el texto según la herramienta.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de hacker con sudadera con capucha - pentesting  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de protección de datos. escaneo de huellas dactilares, sistema de identificación. estilo moderno de dibujos animados planos. ilustración vectorial - personal de seguridad | Por favor un sonido acorde a las animaciones de texto e imágenes y narración | Los ‘*pentesting’* son pruebas que realizan los expertos mediante técnicas avanzadas para detectar posibles amenazas o áreas con puntos débiles que los piratas informáticos pueden aprovechar.  La ‘formación del personal’, aunque no esté catalogada como herramienta tecnológica, es importante, ya que, contar con funcionarios que tengan conocimientos básicos y precavidos al momento de interactuar con las herramientas o dispositivos que almacenan la información es de gran utilidad para mitigar riesgos.  De esta forma, se conocen a detalle las características de las herramientas de seguridad tipo *hardware* y *software*. La invitación ahora es a revisar los manuales técnicos de cada herramienta que se comparten en el siguiente tema de estudio. (510) | *Pentesting*  Pruebas de detección de amenazas  Formación del personal |
| **Nombre del archivo** | **233103\_CF07\_v2.mp3** | | | |

**1.1. Manuales técnicos**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Luego de identificar algunas de las herramientas, es importante conocer también los manuales, cuyo propósito fundamental es lograr parametrizar el *hardware* y *software* útil para los sistemas de seguridad informática, desde su configuración inicial, hasta el monitoreo en red, teniendo en cuenta las especificaciones técnicas, estándares y normas de seguridad que ayudarán al uso e implementación de las herramientas sin importar si hay rotación continua de encargados.  concepto de educación en línea - manuales tecnicos fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i4    En la siguiente tabla se listan las herramientas con el *link* (direcciones web) de acceso a los manuales de cada herramienta descritas en el video anterior. | |

**Tabla 1**

*Lista de herramientas y manuales técnicos*

| **Herramienta** | **Tipo** | **Link de acceso al manual** |
| --- | --- | --- |
| Llaves U2F | Hardware | <https://manuals.plus/es/feitian/epass-fido-nfc-multipass-security-key-manual#user_manual> |
| *Firewall* por *hardware* | Hardware | <https://www.manualpdf.es/cisco/mx67w/manual> |
| *Router* VPN – VPN *Box* | Hardware | <http://downloads.trendnet.com/TW100-BRV214/manual/SP_Web_TW100-BRV214(1.01).pdf> |
| *Hardware* de cifrado | Hardware | <https://www.kingston.com/datasheets/kc600_es.pdf> |
| *Tokens* PKI | Hardware | <https://efirma.com.py/descargas/Manual%20de%20Administracion%20de%20Token%20ME.pdf> |
| Acelerador SSL/TLS | Hardware | <https://www.g-sec.lu/sslaudit/documentation.pdf> |
| Sistema de pago seguro | Hardware | <https://www.banrep.gov.co/sites/default/files/reglamentacion/dsp_158.pdf> |
| Cartera digital | Hardware | <https://www.gov.co/files/Manual%20de%20Usuario_Servicio_CCD_V1.0.2.pdf> |
| Sensores biométricos | Hardware | <https://www.solomon.cl/wp-content/uploads/2019/11/Manual-FPT-153.pdf> |
| Candado | Hardware | <https://www.manuales.com.co/kensington/combination-laptop-lock/manual> |
| Antivirus | Software | <https://support.kaspersky.com/KESWin/11/es-ES/KESWin-11-es-ES.pdf> |
| *Firewall* | Software | <https://www.academia.edu/22360402/Manual_de_Usuario_de_Pfsense_Firewall> |
| *Proxy* | Software | <https://mestreacasa.gva.es/c/document_library/get_file?folderId=500017506371&name=DLFE-1398307.pdf> |
| MDR – *Managed Detection and Response* | Software | <https://www.ciosummits.com/The_Definitive_Guide_to_Managed_Detection_and_Response_MDR.pdf> |
| *Pentesting* | Software | <https://www.researchgate.net/publication/341255054_GUIA_PRACTICA_PARA_PRUEBAS_DE_PENTEST_BASADA_EN_LA_METODOLOGIA_OSSTMM_V21_Y_LA_GUIA_OWASP_V30> |
| Formación del personal | NA | <https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf> |

*Ref. Creación propia del experto temático con ajustes del Diseñador instruccional.*

| Cuadro de texto |
| --- |
| Ya se conocen las herramientas y sus características. Es hora de estudiar los equipos usados para la protección de sistemas. |

**1.2. Configuración básica de equipos**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Los activos de información en una entidad deben ser preservados, y para ello se requiere de protección, ya sea con buenas prácticas de administración o mediante equipos que impidan el acceso no autorizado de usuarios a los repositorios de los mismos. Teniendo en cuenta lo anterior, a continuación, se describe paso a paso la configuración de algunos de los equipos más usados para la protección de los sistemas en las entidades. | |

**Llaves U2F**

| **Tipo de recurso** | Rutas /Pasos Horizontal | |
| --- | --- | --- |
| **Introducción** | Para el uso del t*oken* o llave U2F es necesario realizar dos registros y seguir estos pasos: | |
| **Paso 1** | **1er. Registro**  Verificación en Google   1. Inicie sesión con de google Chrome en una computadora. 2. Haga *click* en ‘mi cuenta’ -> ‘inicio de sesión y seguridad’ -> ‘verificación en dos pasos’. 3. Haga clic en ‘agregar clave de seguridad’ y siga las instrucciones para completar el registro. 4. Se le informará que inserte su llave de seguridad *ePass* FIDO® durante el proceso de registro. 5. Haga *click* / toque el botón para comprobar la presencia del usuario cuando el indicador de autenticación parpadee. Su registro se completará en un momento. | mujer trabajando en un escritorio de pie - registro token fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i5 |
| **Paso 2** | **2do. Registro**  Programa de protección avanzada de Google   1. Acceso: página de inicio de Programa de protección avanzada con un Navegador Chrome: <https://landing.google.com/advancedprotection/> 2. Haga *click* en ‘¡empieza ya!’. 3. Prepare 2 llaves de seguridad y haga clic en ‘tengo 2 llaves de seguridad’. 4. Se le pedirá que ingrese la contraseña otra vez. 5. Registre la clave de seguridad una por una y haga clic en ‘continuar’. 6. Lea y confirme las notificaciones sobre el Programa de protección avanzada y haga clic en ‘encender’. Su registro se completará en un momento. | hombre en casa usando hardware wallet para criptomonedas - token fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i6 |

**Acelerador SSL/TLS**

| **Tipo de recurso** | Carrusel de tarjetas | |
| --- | --- | --- |
| **Introducción** | Los pasos para realizar la configuración de estos aceleradores son: | |
| hombre usando teléfono inteligente móvil, pago en línea, banca y compras en línea en casa. negocios y tecnología. - pago en linea fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i7 | | |
| 1-*Scan*  Ingrese al *host* que va a escanear y el puerto apropiado. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de alojamiento web con personajes de personas. base de datos en línea, servidor, centro de datos web, computación en la nube, tecnología, computadora, seguridad. ilustración vectorial moderna aislada para web, banner, póster, ui - host  **Cod.Imagen:** 233103\_i8 |
| 2-*Clear*  Limpie los resultados. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de botón de teclado trashcan - borrar datos  **Cod.Imagen:** 233103\_i9 |
| 3-*Option*  Solo mostrar conjuntos de cifrado admitidos. | | pago sin contacto en una cafetería - mostrar admitidos fotografías e imágenes de stock    **Cod.Imagen:** 233103\_i10 |
| 4-*Experimental*  Huellas dactilares de motor SSL *engine* (ver ‘*Fingerprint*’ Experimental). | | el escaneo biométrico de huellas dactilares proporciona seguridad protección cibernética. tecnología de internet. seguridad de los datos. protección de datos de información personal. - mostrar admitidos fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i11 |

**Sistema de pago seguro**

| **Tipo**  **de recurso** | Pestañas o tabs horizontales | |
| --- | --- | --- |
| **Introducción** | Para realizar pagos con datáfono de forma segura, tenga en cuenta: | |
| **Autenticación** | El ingreso al sistema de información se debe realizar a través del portal de aplicaciones SEBRA (que hace parte de la plataforma SEBRA). En este portal, el proceso de autenticación fuerte es de múltiple factor (*pin* definido por el usuario y *token* OTP-*One Time Password*). Luego de completar la autenticación en SEBRA, se habilita a través de este el acceso del usuario hacia el CUD mediante un mecanismo de *single-sign-on* (SSO). | **Cod.Imagen:** 233103\_i12 |
| **Control de acceso y autorización** | Existen dos fases de control de acceso: la primera ya descrita en el documento anexo a través del portal SEBRA, y la segunda se realiza al ingresar al sistema CUD a través de su integración con el S3, donde el acceso a las funciones o pantallas está controlado según los roles y perfiles que el delegado de la ‘entidad participante’ haya configurado para el usuario (únicamente se pueden ejecutar las funciones autorizadas por estos). | **Cod.Imagen:** 233103\_i13 |
| **Integridad y confidencialidad** | La comunicación entre los usuarios y el aplicativo se realiza usando protocolos seguros de comunicación (en este caso https con TLS versión X). | **Cod.Imagen:** 233103\_i14 |
| **Observancia** | Las principales acciones de los usuarios, desde la autenticación inicial hasta la captura y aprobación de transferencias de fondos, son almacenadas en tablas de la base de datos del sistema cuya información no puede ser modificada debido a los controles de cambio de datos implementados a través de herramientas de monitoreo, alerta y protección de bases de datos (tecnologías de *database security*). | **Cod.Imagen:** 233103\_i15 |
| **Trazabilidad de las transacciones realizadas en el CUD** | Desde el momento en que se autentica en el sistema, a través del proceso de *single-sign-on* desde el portal SEBRA, el usuario es almacenado en una tabla que registra sus acciones por medio de la acción de ‘inicio de sesión’. | **Cod.Imagen:** 233103\_i16 |
| **Registro** | Los registros de operación de los servicios involucrados en el Portal SEBRA, ‘servicio de autenticación fuerte’ y S3 son conservados en una herramienta de industria que la entidad maneja para este fin. | **Cod.Imagen:** 233103\_i17 |
| **No repudio** | Debido a que todas las acciones realizadas por los usuarios están completamente registradas y protegidas por los esquemas de observancia y auditoría ya descritos, las transacciones hechas a través del sistema cuentan con evidencia digital suficiente para evitar el repudio de estas. | **Cod.Imagen:** 233103\_i18 |

**Sensores biométricos**

| **Tipo de recurso** | Acordeón tipo 1 |
| --- | --- |
| **Introducción** | Es el proceso de comparar la huella que lee el equipo con las huellas almacenadas, luego la identificación de la misma o plantilla correspondiente, y, finalmente, la verificación del usuario que la registró. A continuación se describen los tipos de autenticación: |
| sistema de seguridad de escaneo de huellas dactilares en pared en un edificio de oficinas - sensores biométricos fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i19 | |
| Autentificación (Verificación) 1:1  De este modo, ingresa un número de ID de usuario y luego la huella dactilar correspondiente. Las huellas dactilares asociadas al número de ID serán comparadas 1-1 con la leída. Esta autenticación 1-1 tarda un período de tiempo muy breve, sin importar el número de usuarios registrados. No hay necesidad de hacer modificaciones especiales en la configuración del sistema. | |
| Autentificación (Identificación) 1:  En este modo solo es necesario que el usuario ponga su huella dactilar en el sensor del equipo. Aunque el procedimiento de la autentificación es simple, este método durará un poco más de tiempo que la autentificación 1.1 si hay muchos usuarios registrados. No hay necesidad de hacer ningún ajuste especial en la configuración del sistema. | |
| Autentificación por Clave  Una clave de 1-5 dígitos de largo puede ser usada para validar una autentificación de acceso. Se puede usar este método en casos especiales, como cuando las huellas de un trabajador están muy deterioradas, o el sensor del equipo esté dañado. | |

| Cuadro de texto |
| --- |
| Configuración básica de equipos  Para conocer la configuración de cada uno de los equipos más usados para la protección, se le invita a ver el documento. (Anexo 1)  **Descargar** |

| Cuadro de texto |
| --- |
| Luego de conocer la configuración básica de algunos equipos es momento de conocer cómo se realiza el monitoreo a los mismos. |

**2. Monitoreo de equipos**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| El monitoreo continuo de los equipos que hacen parte de la red de seguridad de la información sigue unos protocolos o procedimientos descritos en la normatividad ISO 27000. Estos deben ser establecidos o personalizados de acuerdo al tipo y necesidad de la empresa. Trae consigo la operación de herramientas que protegen y controlan los activos, así como de aquellas que vigilan y gestionan los incidentes que se puedan presentar.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de icono iso 27000. sistema de gestión de la seguridad de la información. símbolo de calidad estándar. signo de botón vectorial aislado sobre fondo blanco - iso 27000  **Cod.Imagen:** 233103\_i20  El monitoreo se hace a elementos tangibles que requieren de la seguridad física que otorga diversos equipos comerciales; estos están condicionados por el buen funcionamiento de los *firewalls*, *proxy*-caché, redes privadas virtuales, identificadores, firmas, entre otros. De allí que las amenazas serán controladas y los ataques a los sistemas informáticos o instalaciones no causará un daño crítico, lo que permitirá que las operaciones de la entidad no se vean interrumpidas.  diseño de páginas web. desarrollo de tecnologías de programación y codificación. - monitoreo de equipos fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i21 | |

| **Tipo de recurso** | Tarjetas Animadas |
| --- | --- |
| **Introducción** | Existen dos tipos de herramientas a tener en cuenta: |
| hembra hogar propietario de verificar el consumo de energía - herramientas de monitoreo fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i22  Hembra hogar propietario de verificar el consumo de energía. | Herramientas de monitoreo y gestión  Son aquellas que facilitan identificar las deficiencias y necesidades para lograr optimizar la seguridad digital de la empresa de forma eficiente y no reactiva. |
| concepto de ciberseguridad y protección de datos digitales - amenazas seguridad digital fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i23  Concepto de ciberseguridad y protección de datos digitales. | Herramientas de protección y control  Son aquellas que una vez identificadas las necesidades y detectadas las posibles amenazas, proporcionan la seguridad y confiabilidad necesarias para realizar acciones a través de la red, ya que se tendrá la certeza de que activarán cuando se encuentren al frente de una posible vulnerabilidad. |

| Cuadro de texto |
| --- |
| Para conocer con detalle los tiempos de herramientas, a continuación, se realiza una descripción |

**2.1. Herramientas de monitoreo y gestión**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Se debe empezar por definir el monitoreo y gestión en red como la acción que permite aumentar la seguridad, proporcionando información que todas las áreas de Tecnología de la Información, TI, requieren para asegurar un óptimo funcionamiento y aplicar gestión o toma de decisiones precisas en caso de presentar ataques o intentos de acceso no autorizados. Para ello, es indispensable la aplicación o ejecución de herramientas y *software* que detecten deficiencias o necesidades para ser abordadas de manera preventiva y no correctiva, de tal forma que se pueda mantener a salvo la información.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de seguridad de los archivos - informacion protegida  **Cod.Imagen:** 233103\_i24  Seguridad de los archivos. | |

| **Tipo de recurso** | | Pestañas o tabs Verticales |
| --- | --- | --- |
| **Introducción** | | A continuación, se presentan las herramientas de monitoreo de red que actualmente son más efectivas y que tienen un papel protagónico al momento de medir la integridad en la infraestructura TI.  La información descrita se tomó con referencia en la página oficial de SolarWinds (s.f.) |
| agentes especiales de la cia están buscando criminales particularmente peligrosos. gracias a la alta tecnología, pueden rastrear fácilmente la ubicación de cualquier objeto o persona. están muy cerca de resolver este misterioso crimen. - monitoreo y gestion información fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i25 | | |
| *Network Performance*  *Monitor* (NPM) | **Monitoreo de red**  Permite tener una idea precisa del estado de la red *on time*, sin importar la cantidad de proveedores o tipos de redes.   * Suministra el historial de utilización para planificar tu capacidad. * Se generan alertas cuando algo va mal en un sistema crítico. * Soluciones para la nube y las instalaciones siempre disponibles en un solo lugar. * Los firewalls no se van a utilizar en exceso. * Si algún equipo falla se sabrá del incidente al instante, sin importar en donde te encuentres. * Cuenta con Monitoreo, instalación, mantenimiento y seguimiento por parte de *Network Operation Center* (NOC). | |
| *Network Traffic Analyzer* (NTA) | **Monitoreo de tráfico en red**  Permite que la información de la empresa se transmita sin problemas, evitando cuellos de botella y asumiendo el control total de la red. Realiza Monitoreo *on time* (tiempo real) del ancho de banda mediante el análisis de tráfico, visualizando el desempeño de cada sección analizada.   * Monitorea el uso del ancho de banda por aplicación, protocolo y grupo de direcciones IP. * Recibe alertas si el tráfico de la aplicación de repente aumenta, disminuye o desaparece por completo. * Analice los patrones del tráfico de red a lo largo de meses, días o minutos al explorar cualquier elemento de la red en profundidad. * Cuenta con compatibilidad de conmutadores distribuidos de *VMware vSphere.* * Correlaciona datos de red de apilamiento cruzado de *PerfStack*™. | |
| *Server and Application Monitor* (SAM) | **Monitoreo de aplicaciones**  Software que monitorea los sistemas informáticos, aplicaciones y servidores. Debido a su versatilidad, permite la puesta en marcha en cuestión de minutos con infinitas posibilidades de personalización.   * Monitorea todo tu entorno de servidores locales, nube o aplicaciones híbridas y tu infraestructura con una sola herramienta. * Más de 1200 plantillas de monitoreo de infraestructuras, sistemas y aplicaciones. * Monitoreo integral de las aplicaciones de Microsoft, los sistemas, el hipervisor, y los productos IaaS, PaaS y SaaS. * Visualiza y asigna las relaciones basadas en comunicaciones dinámicas entre aplicaciones y servidores para detectar problemas de red que disminuyen la velocidad de tus aplicaciones. | |

| Cuadro de texto |
| --- |
| Es momento de pasar a las herramientas de protección y control. |

**2.2. Herramientas de protección y control**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| En el génesis de la era digital los ataques cibernéticos eran técnicamente poco sofisticados, pero con el paso del tiempo, se han desarrollado métodos más complejos, que buscan ‘agujeros negros’ en los sistemas operativos. Estos existen en todos y hacen referencia a errores en la configuración. Para que un sistema esté completamente protegido, requiere de la implementación y buen uso de una mezcla de diversas herramientas existentes en el mercado, ya que no existe ninguna que proteja al 100%. | |

| **Tipo de recurso** | Acordeón tipo 2 |
| --- | --- |
| **Introducción** | A continuación, se detallan las herramientas más usadas para la protección y control del sistema que almacena la información y la red de una empresa: |
| sistemas digitales de seguridad en segundo plano y protección de datos - seguridad digital fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i26 | |
| *Next Generation Firewall* (NGF)  Sistema, o conjunto de sistemas, que se sitúan entre 2 redes y establecen una política de seguridad, que consiste en proteger una red privada de otra red poco confiable, como por ejemplo el internet.  Acción: bloquear acceso a redes no confiables mediante filtros previamente establecidos por el administrador de los sistemas (Microsoft Ignite, s.f.) | |
| *Proxy*-cache  Servidor situado entre el del usuario y otra red externa (internet) actuando como protector al separar las redes y acelerar el acceso a páginas web.  Acción: restringir los contenidos de diversas páginas como, por ejemplo: contenido para adultos, *pop up*, ventanas emergentes. (Microsoft Ignite, s.f.) | |
| Filtrado de contenidos  Sistema automatizado para el procesamiento de grandes volúmenes de datos aplicando acciones a los contenidos que cumplen criterios específicos.  Acción: controlar el contenido que se pueda desplegar en las páginas visitadas. (Microsoft Ignite, s.f.) | |
| *Access Control List* ACL  Grupo de reglas establecidas de acuerdo a preferencia en el tráfico de redes. Las reglas incluyen el direccionamiento IP de origen y destino, el puerto del paquete.  Acción: permitir o denegar el tráfico que ingresa o sale de una red. (Microsoft Ignite, s.f.) | |
| Redes Privadas Virtuales VPN  Es una conexión cifrada a Internet que se hace a través de un dispositivo a una red (por ejemplo, internet).  Acción: permitir que los usuarios trabajen de forma remota y que se espíe el tráfico de la red por personas no autorizadas. (Microsoft Ignite, s.f.) | |
| *Intrusion Detection System* IDS  Aplicación que detecta el acceso no autorizado a un ordenador o a una red.  Acción: monitorear el tráfico entrante de una red para ser comparado con una base de datos en continua actualización, en donde se encuentra una la lista de diversas amenazas. (Microsoft Ignite, s.f.) | |
| *Intrusion Prevention System* IPS  Sistema con actividad preventiva, ya que protege los sistemas de ataques e intrusiones.  Acción: analizar *on time* todas las conexiones y protocolos para determinar si se produce o se va a producir un incidente. (Microsoft Ignite, s.f.) | |
| *Web Application Firewall* WAF  Sistema que actúa como intermediario entre usuarios y aplicaciones web, que se rigen por un conjunto de reglas previamente definidas.  Acción: controlar las comunicaciones HTTP (solicitud-respuesta) y analizarlas antes de conectar con los usuarios o aplicaciones externas. (Microsoft Ignite, s.f.) | |

| Cuadro de texto |
| --- |
| Ya se estudiaron las herramientas, es hora de conocer cómo gestionarlas y dar respuestas a los incidentes asociados a riesgos y amenazas en contra de los datos e información de la organización. |

**3. Respuesta a incidentes**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Las brechas de seguridad pueden causar pérdida de datos, paralizar la operatividad de una empresa, ocasionar la pérdida de confianza por parte de los usuarios, e, incluso, llevar a multas y problemas regulatorios. Para evitar todo lo anterior existe la respuesta a incidentes, la cual es la reacción que se tiene ante posibles amenazas de TI, vulnerabilidades de seguridad y/o tiempo en que el servidor esté inactivo. Esto se lleva a cabo a través de la implementación de herramientas y controles básicos, la validación de su funcionalidad y la verificación del cumplimiento de las cadenas de custodia, según procedimientos técnicos de la política de seguridad de la organización.  dos programadores profesionales de ti que analizan el diseño y el desarrollo de la arquitectura de red de datos de blockchain se muestran en la pantalla del equipo de escritorio. departamento técnico de centros de datos de trabajo con racks de servidores - respuesta a incidentes fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i27  En el siguiente gráfico se describen las acciones necesarias para responder de forma efectiva a los incidentes. | |

| **Tipo de recurso** | Infografía interactiva Punto caliente | |
| --- | --- | --- |
| **Texto introductorio** | Dentro de las acciones que se deben tomar se destacan: | |
| **Nota:** Fuente. Elaboración propia del experto. | | |
| **Código de la imagen** | **Cod.Imagen:** 233103\_i28 | |
| **Punto caliente 1** | Monitorear y verificar: realizar monitoreo y verificación de los elementos de control con el fin de detectar un posible incidente de seguridad de la información. | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 2** | Copias de seguridad: generar copias de seguridad de los tipos incremental, diferencial y total. | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 3** | Plataformas de auditorías de *logs*: implementar plataformas de auditorías de *logs* nist sp 800-92, correlacionadores de eventos, revisión de patrones de ataque, metodologías, revisión de archivos de *logs.* | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 4** | Clasificación de los ataques: clasificar los ataques de acuerdo a su gravedad.   * + Gravedad 1: Incidente crítico con elevada repercusión.   + Gravedad 2: Incidente grave con considerable repercusión.   + Gravedad 3: Incidente leve de baja repercusión. | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 5** | Documentar las incidencias: se deben documentar los incidentes a través de un lenguaje que toda la organización pueda comprender | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 6** | Informar a los clientes: comunicarse con los clientes ante cualquier eventualidad de riesgo. | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 7** | Notificar a tiempo: entregar información real y transparente a los clientes que han sido vulnerados. | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 8** | Marco de trabajo: establecer un manual de trabajo con funciones definidas para dar respuesta a incidentes generados. | El punto debe ir en el ícono que corresponda al título |
| **Punto caliente 9** | Solución de incidentes: resolver el incidente y comunicar las acciones tomadas y los niveles de gravedad al que fue expuesta la información. | El punto debe ir en el ícono que corresponda al título |

| **Tipo de recurso** | Rutas / Pasos. Verticales 1 |
| --- | --- |
| **Introducción** | De este modo, las empresas pueden sobrellevar estos incidentes, asumiendo los desafíos de la siguiente manera: |
| ilustraciones, imágenes clip art, dibujos animados e iconos de stock de protección de datos de privacidad, plantilla de página de aterrizaje de red privada virtual de internet. personajes diminutos alrededor de enorme portátil - seguridad digital  **Cod.Imagen:** 233103\_i29 | |
| **Botón 1** | Con procedimientos de respuesta a incidentes  Creando los procedimientos de respuesta a incidentes, que sean aplicables, medibles, cíclicos y propios, en lugar de subcontratar auditorías externas. |
| **Botón 2** | Tener como prioridad  Comunicar, coordinar y colaborar en todos los aspectos que se requiera ante posibles vulnerabilidades y riesgos latentes. |
| **Botón 3** | Usar herramientas tecnológicas  Hacer uso de las herramientas tecnológicas confiables y posicionadas en el mercado para que el trabajo del equipo tenga respuestas oportunas y preventivas, en lugar de reactivas y tardías. |

| Cuadro de texto |
| --- |
| Luego de conocer los desafíos para dar respuesta efectiva a incidentes, es necesario realizar la validación y el control de seguridad como se describe en el siguiente *ítem.* |

**3.1. Validación de controles de seguridad**

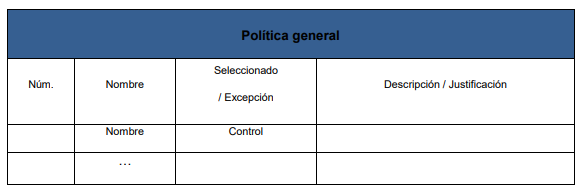
| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Al validar los controles de seguridad se busca proteger y resguardar los activos digitales, sistemas, equipos y datos relacionados con el uso de las TI de los accesos, o intentos de acceso, no autorizados, que puedan causar daños irreparables o corrupción de los archivos.  El propósito de la seguridad informática es proteger la información de las amenazas latentes y sofisticadas que en la actualidad circulan por la red, sin embargo, como ya se sabe, todas las empresas están expuestas a ataques, y la finalidad es paliar las consecuencias al menor grado posible.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de hombre de negocios fuera de una computadora con un escudo - seguridad digital  **Cod.Imagen:** 233103\_i30 | |

| **Tipo de recurso** | Infografía estática |
| --- | --- |
| **Texto introductorio** | La seguridad de la información debe procurar preservar y garantizar el acceso solo a personas autorizadas, que cuenten con privilegios de consulta y modificación establecidos; mantener la integridad y disponibilidad de los datos, salvaguardando su exactitud, los medios de procesamiento y acceso permanente.  Para que esto se cumpla, se requiere de controles de seguridad, como son: |
| <https://img.freepik.com/vector-gratis/plantilla-infografia-negocios_1152-137.jpg?w=740&t=st=1664758558~exp=1664759158~hmac=bf981e1427743903258356279bfdeab5b690abd1e881133d5af269fbfa616ca7>  **Texto de la imagen para diseñador gráfico:**   * Políticas y planes de seguridad TI. * Controlar las operaciones informáticas. * Controlar la gestión de seguridad personal. * Controlar la seguridad del usuario final. * Definir y asignar perfiles de acceso y contraseñas. * Validar diferentes métodos de validación personal. * Definición y asignación de roles y funciones en la organización. * Establecer y monitorear sucesos o eventualidades, para definir un patrón de posible ataque y documentar las formas de contrarrestarlo. * Definir y aplicar las Políticas de Seguridad de TI. | |
| **Código de la imagen** | **Cod.Imagen:** 233103\_i31 |

| Cuadro de texto |
| --- |
| De la guía No. 8 del Ministerio de Tecnologías de la Información y las Comunicaciones, MinTic, ‘Controles de Seguridad y Privacidad de la Información’ (2022) se puede extraer el formato guía de controles estructurados de acuerdo a la tabla que se muestra en la imagen: |

**Tabla 2**

*Controles de seguridad y privacidad de la información*



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (2022) Recuperado de  [https://www.mintic.gov.co/gestionti/615/articles-5482\_G8\_Controles\_Seguridad.pdfl](https://www.istockphoto.com/es/foto/concepto-innovador-de-ciencias-de-la-computaci%C3%B3n-ingeniero-de-software-de-pie-y-gm1355638841-430063743?phrase=respuesta%2Ba%2Bincidentes%2Bde%2Bseguridad%2Bdigital)

**Texto para diseñador web**

Política General

Núm.

Nombre

Nombre

…

Seleccionado/Excepción

Control

Descripción / Justificación

| **Tipo de recurso** | Tarjetas Avatar | |
| --- | --- | --- |
| **Introducción** | Cada campo de la tabla 2 se define a continuación: | |
| Núm.  Este campo identifica cada uno de los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001. | | **Cod.Imagen:** 233103\_i32  [https://www.mintic.gov.co/gestionti/615/articles-5482\_G8\_Controles\_Seguridad.pdfl](https://www.istockphoto.com/es/foto/concepto-innovador-de-ciencias-de-la-computaci%C3%B3n-ingeniero-de-software-de-pie-y-gm1355638841-430063743?phrase=respuesta%2Ba%2Bincidentes%2Bde%2Bseguridad%2Bdigital) |
| Nombre  Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida. | | **Cod.Imagen:** 233103\_i33  [https://www.mintic.gov.co/gestionti/615/articles-5482\_G8\_Controles\_Seguridad.pdfl](https://www.istockphoto.com/es/foto/concepto-innovador-de-ciencias-de-la-computaci%C3%B3n-ingeniero-de-software-de-pie-y-gm1355638841-430063743?phrase=respuesta%2Ba%2Bincidentes%2Bde%2Bseguridad%2Bdigital) |
| Control  Este campo describe el control que se debe implementar con el fin de dar cumplimiento a la política definida. | | **Cod.Imagen:** 233103\_i34  [https://www.mintic.gov.co/gestionti/615/articles-5482\_G8\_Controles\_Seguridad.pdfl](https://www.istockphoto.com/es/foto/concepto-innovador-de-ciencias-de-la-computaci%C3%B3n-ingeniero-de-software-de-pie-y-gm1355638841-430063743?phrase=respuesta%2Ba%2Bincidentes%2Bde%2Bseguridad%2Bdigital) |
| Seleccionado / Excepción  El listado de controles además debe ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado, tanto si se implementa, como si se excluye de hacerlo, lo cual ayuda a que la entidad tenga documentado y de fácil acceso el inventario de controles. | | **Cod.Imagen:** 233103\_i35  [https://www.mintic.gov.co/gestionti/615/articles-5482\_G8\_Controles\_Seguridad.pdfl](https://www.istockphoto.com/es/foto/concepto-innovador-de-ciencias-de-la-computaci%C3%B3n-ingeniero-de-software-de-pie-y-gm1355638841-430063743?phrase=respuesta%2Ba%2Bincidentes%2Bde%2Bseguridad%2Bdigital) |
| Descripción / Justificación  El listado de controles cuenta con la descripción de cada uno. Adicionalmente, es posible utilizarlo para la generación de la declaración de aplicabilidad, donde son justificados, bien sea porque se implementen o no. | | **Cod.Imagen:** 233103\_i36  [https://www.mintic.gov.co/gestionti/615/articles-5482\_G8\_Controles\_Seguridad.pdfl](https://www.istockphoto.com/es/foto/concepto-innovador-de-ciencias-de-la-computaci%C3%B3n-ingeniero-de-software-de-pie-y-gm1355638841-430063743?phrase=respuesta%2Ba%2Bincidentes%2Bde%2Bseguridad%2Bdigital) |

| Cuadro de texto |
| --- |
| **Controles de Seguridad y Privacidad de la Información**  Para ampliar la información sobre Controles de Seguridad y Privacidad de la Información, por favor remítase al Anexo 2 págs. 9-17 (Guía No. 8 - Controles de Seguridad y Privacidad de la Información).  **Descargar** |

| Cuadro de texto |
| --- |
| Para continuar con el estudio de los elementos para dar respuesta a incidentes, es hora de ver las cadenas de custodia. |

**3.2. Cadenas de custodia**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Las cadenas de custodia en los sistemas de seguridad de la información permiten la gestión oportuna, ordenada y efectiva de los incidentes y eventualidades que puedan llegar afectar la transparencia, integridad, confidencialidad, y disponibilidad de los activos de información en las empresas, aplicando acciones preventivas y correctivas que minimicen los impactos al nivel más bajo posible. Los pasos para diseñar una cadena de custodia son:   * Identificación, registro y clasificación. * Control y restauración. * Erradicación, análisis e investigación. * Cierre y activación.     logista pharma con iot basado en blockchain - cadenas de custodia fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i37 | |

| Cuadro de texto |
| --- |
| En la Tabla 3 se detalla cómo actúa en cada paso la cadena de custodia. |

**Tabla 3.**

*Pasos para diseñar una cadena de custodia*

| **PASOS** | **ACTÚA SOBRE** |
| --- | --- |
| Identificación, registro y clasificación | Incidente o evento de seguridad |
| Control y restauración | Efectos negativos y daños |
| Erradicación, análisis e investigación | Evento, incidente y causas |
| Cierre y activación | Incidente y procedimiento para la administración del plan de mejoramiento |

*Nota.* Esta tabla se realiza con la información de la página oficial de Función Pública. Recuperado de <https://www.funcionpublica.gov.co/documents/34645357/34703090/Guia_gestion_incidente_seguridad_informacion.pdf/e2cd6309-a097-0598-8988-f2b2c3f039f4?t=1607031995675>

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Estas acciones son llevadas a cabo por el equipo conformado para dar respuesta a incidentes de la SI (ERISI). Este, es el responsable de accionar las respuestas en el momento de presentarse eventos o incidentes que puedan afectar la transparencia, confidencialidad, integridad y disponibilidad de los activos digitales. El ERISI puede estar conformado por los siguientes perfiles:   * Profesionales con amplio conocimiento en hardware, software y/o redes. * Profesionales de Bases de Datos. * Líderes de sistemas de información. * Representantes misionales. * Representantes del área directiva de la Entidad.   profesional ingenieros trabajando en el centro de control de sistema completo de monitores y servidores. supervisor tiene laptop y lleva a cabo una reunión informativa. posiblemente la agencia gubernamental realiza investigación. - equipo seguridad digital fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i38 | |

| Cuadro de texto |
| --- |
| EL grupo ERISI clasifica los incidentes y/o eventos de seguridad de acuerdo a la siguiente escala: |

**Tabla 4.**

*Clasificación de incidentes y/o eventos de seguridad*

| **NIVEL** | **VALOR DEL ACTIVO** | **TIEMPO DE ATENCIÓN** |
| --- | --- | --- |
| Extremo | 17 | 1 Hora |
| Muy Alto | 15 – 16 | 6 Horas |
| Alto | 12 – 14 | 12 Horas |
| Medio | 9 – 11 | 2 Días |
| Bajo / Despreciable | < 9 | 1 Semana |

*Nota.* Esta tabla se realiza con la información de la página oficial de Función Pública. Recuperado de <https://www.funcionpublica.gov.co/documents/34645357/34703090/Guia_gestion_incidente_seguridad_informacion.pdf/e2cd6309-a097-0598-8988-f2b2c3f039f4?t=1607031995675>

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Para que el equipo ERISI establezca la prioridad o el tiempo de atención del incidente, es indispensable que se remitan al inventario de activos de información y en la columna ‘valor del activo’ y comprobar dicha información; solo así, es posible determinar la prioridad de atención del evento.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ciberseguridad, contraseñas seguras y registro del sitio. - equipo seguridad digital  **Cod.Imagen:** 233103\_i39 | |

| Cuadro de texto |
| --- |
| Guía para gestionar incidentes de SI\_Función Pública.  Para ampliar la información sobre cadenas de custodia, por favor remítase al Anexo 3\_Guia para gestionar incidentes de SI\_Funcion Pública.  **Descargar** |

| Cuadro de texto |
| --- |
| Para continuar con la exploración de los demás recursos que se encuentran disponibles en este componente formativo, es necesario dirigirse al menú principal, en donde encontrará la síntesis, una actividad didáctica, material complementario, entre otros.  ¡Éxitos en este camino de aprendizaje! |

**SÍNTESIS**

| **Tipo de recurso** | Síntesis |
| --- | --- |
| Control de la seguridad digital  Síntesis: Ciberseguridad, herramientas de monitoreo y control | |
| **Introducción** | Como refuerzo a continuación, encontrará la síntesis del componente formativo de una forma gráfica, así podrá repasar las diferentes temáticas tratadas en el mismo. |
| **Cod.Imagen:** 233103\_i40  **Nota:** Fuente. Elaboración experto.  Texto para diseñador web  **ERISI** - Equipo de Respuesta a Incidentes de Seguridad de la Información  **REQUIERE**   * **HERRAMIENTAS DE CONTROL DE SI -** *Next Generation Firewall* (NGF), *Proxy*-cache, Filtrado de contenidos, *Access Control List* ACL, Redes Privadas Virtuales VPN, *Intrusion Detection System* IDS, *Intrusion Prevention System* IPS, *Web Application Firewall WAF*.   **ACCION 1**   * **Monitoreo de equipos**    + Herramientas de monitoreo y gestión - *Network Performance Monitor* (NPM), *Network Traffic Analyzer* (NTA), *Server and Application Monitor* (SAM).   + Herramientas de protección y control - *Next Generation Firewall* (NGF), *Proxy*-cache, Filtrado de contenidos, *Access Control List* ACL, Redes Privadas Virtuales VPN, *Intrusion Detection System* IDS, *Intrusion Prevention System* IPS, *Web Application Firewall* WAF.   **ACCION 2**   * **Respuesta a incidentes**   + Validación de controles de seguridad, políticas y planes de seguridad TI, controlar las operaciones informáticas, controlar la gestión de seguridad personal, controlar la seguridad del usuario final, definir y asignar perfiles de acceso y contraseñas, validar diferentes métodos de validación personal, definir y asignar de roles y funciones en la organización, establecer y monitorear sucesos o eventualidades, para definir un patrón de posible ataque y documentar las formas de contrarrestarlo, definir y aplicar las políticas de seguridad de TI.   + Cadenas de custodia - Identificación, registro y clasificación, control y restauración, erradicación, análisis e investigación, cierre y activación.   **ACCION 3**   * **Gestión de hardware y software**   + Configuración básica de equipos - Equipos que impiden el acceso no autorizado de usuarios a los repositorios de los activos.   + Manuales técnicos - Llaves U2F, *firewall* por *hardware,* *router* VPN – VPN Box, *hardware* de cifrado, *tokens* PKI, Acelerador SSL/TLS, Sistema de pago seguro, cartera digital, sensores biométricos, candado, Antivirus, *firewall*, *proxy*, MDR – *Managed Detection and Response*, *pentesting*, formación del personal. | |

**Relación de conceptos**

| **Tipo de recurso** | Actividad didáctica. Arrastrar y soltar | |
| --- | --- | --- |
| Llegó el momento de validar los aprendizajes adquiridos con el estudio del componente formativo.  Por favor relacionar cada término con la definición, arrastrando y soltando donde corresponda. | | datos de gráficos de pronóstico financiero, marketing de planificación financiera, hombre de negocios que trabaja en la bolsa de valores cripto blockchain análisis de datos de inversión comercial. seminario web de reuniones en línea consulta de negoc - herramientas ciberseguridad fotografías e imágenes de stock  **Cod.Imagen:** 233103\_i41 |
| El \_\_\_\_\_\_\_\_\_ y la masificación del uso de las Tecnologías de la Información y las Comunicaciones (TIC) ha incrementado los usuarios digitales en todos los sectores de la economía.  Retro+ Felicitaciones, has comprendido la temática de la sección 1 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 1 del componente formativo. | | Internet |
| El propósito fundamental de los \_\_\_\_\_\_\_\_\_\_\_ es lograr parametrizar el *hardware* y *software* útil para los sistemas de seguridad informática, desde su configuración inicial, hasta el monitoreo en red.  Retro+ Felicitaciones, has comprendido la temática de la sección 1.1 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 1.1 del componente formativo. | | Manuales |
| Sistema que proporciona certificados digitales, además de claves privadas.  Retro+ Felicitaciones, has comprendido la temática de la sección 1.1 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 1.1 del componente formativo. | | *Token* PKI |
| Se usan como control de acceso a lugares donde está almacenada la información; si el usuario no es reconocido por el sensor, el acceso al sitio será denegado.  Retro+ Felicitaciones, has comprendido la temática de la sección 1.1 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 1.1 del componente formativo. | | Sensores biométricos |
| Programa o dispositivo físico que actúa de intermediario entre conexiones del navegador e internet, filtrando todos los paquetes entre ambos.  Retro+ Felicitaciones, has comprendido la temática de la sección 1.1 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 1.1 del componente formativo. | | *Proxy* |
| No está catalogada como herramienta tecnológica, pero es importante contar con funcionarios que tengan conocimientos básicos y precavidos al momento de interactuar con las herramientas o dispositivos que almacenan la información.  Retro+ Felicitaciones, has comprendido la temática de la sección 1.1 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 1.1 del componente formativo. | | Formación del personal |
| Se hace a elementos tangibles que requieren de la seguridad física que otorgan diversos equipos comerciales.  Retro+ Felicitaciones, has comprendido la temática de la sección 2 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 2 del componente formativo. | | Monitoreo de equipos |
| Para que un sistema esté completamente protegido requiere de la implementación y buen uso de una mezcla de diversas herramientas existentes en el mercado, ya que no existe ninguna que proteja al 100% los sistemas.  Retro+ Felicitaciones, has comprendido la temática de la sección 2.2 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 2.2 del componente formativo. | | Herramientas de protección y control |
| Reacción que tiene una empresa ante posibles amenazas de TI, vulnerabilidades de seguridad y/o tiempo en que el servidor esté inactivo.  Retro+ Felicitaciones, has comprendido la temática de la sección 3 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 3 del componente formativo. | | Respuesta a incidentes |
| Se busca proteger y resguardar los activos digitales, sistemas, equipos y datos relacionados con el uso de las TI de los accesos o intentos de acceso no autorizados, que puedan causar daños irreparables o corrupción de los archivos.  Retro+ Felicitaciones, has comprendido la temática de la sección 3.1 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 3.1 del componente formativo. | | Validación de controles de seguridad |
| Permiten la gestión oportuna, ordenada y efectiva de los incidentes y eventualidades que puedan llegar a afectar la transparencia, integridad, confidencialidad, y disponibilidad de los activos de información  Retro+ Felicitaciones, has comprendido la temática de la sección 3.2 del componente formativo.  Retro- Respuesta incorrecta, por favor revisar sección 3.2 del componente formativo. | | Cadenas de custodia |

RESULTADOS:

**>= 7/10** – FELICITACIONES – Tiene claro los conceptos básicos de la gestión de *hardware* y *software*, monitoreo de equipos, y respuesta a incidentes que se pueden presentar en los sistemas o redes de información.

**< 7/10** – Estimado aprendiz, es importante repasar nuevamente el contenido del componente formativo, los conceptos de manuales técnicos, configuración básica de equipos, herramientas de monitoreo y gestión, herramientas de protección y control, validación de controles de seguridad, y cadenas de custodia, ya que no se ha comprendido en su totalidad.

**MATERIAL COMPLEMENTARIO**

| Tipo de recurso | Material complementario | | |
| --- | --- | --- | --- |
| Tema | Referencia APA del material | tipo | Enlace |
| Evaluación del rendimiento de cortafuegos basados en software libre | Perdigón Llanes, R. (2022) Evaluación Del Rendimiento De Cortafuegos Basados En Software Libre."N*OVASINERGIA 5*(1) p. 31-42. | Articulo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_doaj_primary_oai_doaj_org_article_43539a8d908740c09c11297e9b1b872a> |
| Gestión de incidentes de seguridad informática (MF0488\_3) | Chicano Tejada, E. (2014). *Gestión De Incidentes De Seguridad Informática.* IC Editorial | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_elibroELB44101> |
| Herramientas para la seguridad: de como un paquete de trucos tecnológicos puede mejorar, pero no garantizar, su seguridad. | The Economist (2003) Herramientas para la seguridad: de como un paquete de trucos tecnológicos puede mejorar, pero no garantizar, su seguridad. En *Gestión de TI.*  (p. VI-IX*) Nexos. Sociedad, ciencia y literatura S.A.* 25 (310) | Capítulo de artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_gale_lrcgauss_A110619588> |
| Human Factors Approach to Cybersecurity Teamwork – The Military Perspective | Hámornik B.P & Krasznay C. (2019) Human Factors Approach to Cybersecurity Teamwork The Military Perspective. A*dvances in Military Technology.* (14)2 p. 291-305 | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_virtualprovpro21063> |

**GLOSARIO**

| **Tipo de recurso** | **Glosario** |
| --- | --- |
| Acelerador SSL/TLS | *Secure Sockets Layer* (SSL) son protocolos criptográficos que se utilizan con certificados de confianza para garantizar que la comunicación en las redes sea segura. |
| Antivirus | permiten contar con medidas de protección efectivas cuando el equipo se encuentre expuestos a *software* malicioso o cualquier otro tipo de *malware.* |
| Candado universal para portátil | candado con cable de seguridad utilizado para anclar los laptop en un lugar fijo. |
| Cartera digital | también conocida como e*-wallet,* es una espacio virtual donde se almacenan datos bancarios, tarjeta de crédito, entre otros. |
| *Firewall* | sistema para prevenir y proteger la red privada de ataques de otras redes. |
| *Firewall* por *hardware* | unidad física tipo *box* que protege la red de amenazas externas. El dispositivo se instala entre el servidor de la empresa y el internet, permitiendo o denegando el acceso de datos según condiciones específicas del usuario. |
| Formación del personal | aunque no esté catalogada como herramienta tecnológica, es importante contar con funcionarios que tengan conocimientos básicos y precavidos al momento de interactuar con las herramientas o dispositivos que almacenan la información. |
| *Hardware* de cifrado | procesador que maneja cifrado de los datos mediante clave pública o privada. Su función es alojar algoritmos que permiten cifrado o descifrado de esos datos. |
| Llave U2F | unidad USB de doble autenticación que permite generar claves para ingreso seguros es diversos lugares, la persona que no posea esta llave, no podrá vulnerar las cuentas del propietario. |
| MDR – *Managed Detection and Response* | es un servicio en seguridad avanzado, donde se proporciona la búsqueda de amenazas y monitoreo inteligente de las mismas. |
| *Pentesting* | Pruebas que realizan los expertos mediante técnicas avanzadas para detectar posibles amenazas o áreas con puntos débiles que los piratas informáticos pueden aprovechar. |
| *Proxy* | programa o dispositivo físico, que actúa de intermediario entre conexiones del navegador e internet, filtrando todos los paquetes entre ambos. |
| *Router* VPN – VPN *Box* | dispositivo que soporta redes virtuales privadas (VPN) con el propósito de redirigir el tráfico de internet a través de redes privadas seguras. |
| Sensores biométricos | son sistemas mecánicos o electrónicos que se usan para leer o capturar las huellas dactilares. En ciberseguridad, los sensores biométricos se usan como control de acceso a lugares donde está almacenada la información; si el usuario no es reconocido por el sensor, el acceso al sitio será denegado. |
| Sistema de pago seguro | pago electrónico a través de tarjetas físicas mediante datafonos que pueden soportar banda magnética, chip, o tarjeta de proximidad. |
| Tokens PKI | *Public Key Infrastructure* (infraestructura de clave pública), es un sistema que proporciona certificados digitales, además de claves privadas. |

**REFERENTES BIBLIOGRÁFICOS**

| **Tipo de recurso** | Bibliografía |
| --- | --- |
| Banco de la República (2022) Manual de sistemas de pago circular externa operativa y de servicios. DSP -158. | |
| Boronat Pérez, A. (s.f.) Servidor proxy caché squid. | |
| Cárdenas, A., Galvis, A., Ospina J. y Perez, R. (s.f.) *Manual de Usuario de Pfsense Firewall.* Sense FreeBSD | |
| Cisco (s.f.) Manual Cisco MX67W. | |
| Chicano Tejada, E. (2014). *Gestión de incidentes de seguridad informática.* IC Editorial | |
| Departamento Administrativo de Función Pública -DAFP (2020) Guía para gestionar incidentes de seguridad de la información. Proceso de Tecnologías de la Información. | |
| EFirma (2016) Guía de uso. Administración de Token ME Bit4id - PKI Manager. | |
| Esentire (s.f.) The Definitive Guide to Managed Detection and Response (MDR). | |
| Garzón, J. & Gaviria Valencia, R. (2015) Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0 | |
| Hámornik B.P & Krasznay C. (2019) Human Factors Approach to Cybersecurity Teamwork The Military Perspective. A*dvances in Military Technology.* (14)2 p. 291-305 | |
| Hapag-Lloyd (s.f.) Manual de la llave de seguridad ePass FIDO-NFC MultiPass. <https://manuals.plus/es/feitian/epass-fido-nfc-multipass-security-key-manual#user_manual> | |
| Kaspersky (2020) Kaspersky Endpoint Security para Windows. AO Kaspersky Lab | |
| Kaspersky (s.f.) Ransomware: los ataques más resonantes. <https://latam.kaspersky.com/resource-center/threats/top-ransomware-2020> | |
| Kensington (s.f.) Kensington Combination Laptop Lock manual | |
| Kingston (s.f.). Unidad con autocifrado basada en hardware con NAND TLC 3D. | |
| Microsoft Ignite (s.f.) Servidor de red de Microsoft SMB v1: firmar digitalmente las comunicaciones (siempre). <https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/smbv1-microsoft-network-server-digitally-sign-communications-always> | |
| Ministerio de Tecnologías de la Información y las Comunicaciones – MinTic (2022) Guía No 8. Controles de Seguridad y Privacidad de la Información | |
| Organización de Estados Americanos -OEA (2016) Buenas Prácticas para establecer un CSIRT nacional. | |
| Perdigón Llanes, R. (2022) Evaluación Del Rendimiento De Cortafuegos Basados En Software Libre."N*OVASINERGIA 5*(1) p. 31-42. | |
| Satizibal, J. (2020) Manual de usuario carpeta ciudadana digital. Agencia Nacional Digital. | |
| SolarWinds, (s.f.) Innovar la TI. <https://www.solarwinds.com/es/> | |
| Solomon, 2018. Reloj Control FPT MANUAL DE USUARIO TERMINAL FPT Biométrico Reloj Control FPT-153. Recuperado de <https://www.solomon.cl/wp-content/uploads/2019/11/Manual-FPT-153.pdf> | |
| The Economist (2003) Herramientas para la seguridad: de como un paquete de trucos tecnológicos puede mejorar, pero no garantizar, su seguridad. En *Gestión de TI.*  (p. VI-IX*) Nexos. Sociedad, ciencia y literatura S.A.* 25 (310) | |
| Trendnet, 2022. TW100-BRV214. Recuperado de <http://downloads.trendnet.com/TW100-BRV214/manual/SP_Web_TW100-BRV214(1.01).pdf> | |
| Zoller, T (s.f.) SSL Audit – TLS / SSL Scanner. G-SEC | |

# **CONTROL DEL DOCUMENTO**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor (es)** | Abel Fernando Becerra | Experto Temático | Innovate Education | Septiembre/2022 |
| Magda Melissa Rodríguez Celis | Diseñador instruccional | Septiembre/2022 |

**CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)**

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