Guion para desarrollo de contenidos

**Datos de identificación del programa de formación**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Control de la Seguridad Digital |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501111. Control de la seguridad de la información digital | RESULTADOS DE APRENDIZAJE | 220501111-01-Recopilar información de incidentes de seguridad digital según criterios técnicos, marcos de referencia y modelo del negocio |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 05 |
| NOMBRE DEL COMPONENTE FORMATIVO | Ciberseguridad, Generalidades y aplicaciones |
| BREVE DESCRIPCIÓN | Clasificar y almacenar los datos es cada vez más importante, se deben considerar diversas técnicas, análisis y normas que aporten al crecimiento de la organización. La manipulación de volúmenes de datos trae consigo un alto grado de responsabilidad en seguridad, clasificación, conservación y no duplicación de los datos recolectados, exigiendo que se respeten y monitoreen los riesgos que pueden presentarse. |
| PALABRAS CLAVE | Ciberseguridad. *hardware*. Incidente. seguridad digital. *software* |

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

# **TABLA DE CONTENIDOS**

**Introducción**

**1.** **Generalidades de la ciberseguridad**

**2.** **Aplicación de ciberseguridad**

**INTRODUCCIÓN -**

|  |
| --- |
| Cuadro de texto |
| Apreciado aprendiz, bienvenido a este componente formativo, donde se reconocen las generalidades de la ciberseguridad, la normativa, las funciones, procesos de gestión y reportes, para que se puedan aplicar en las empresas mediante herramientas de *hardware y software*; de este modo es necesario estudiar los fundamentos esenciales asociados a eventos e incidentes.  En el siguiente video conocerá, de forma general, la temática que se estudiará a lo largo del componente formativo.  **Ciberseguridad**  Ciberseguridad, empresas, tecnología, red de Internet, desarrollo de software, concepto de protección de datos digitales. Empresario trabajando en un ordenador portátil en la oficina con un sistema antivirus emergente  Imágenes asociadas a la seguridad digital, computadores con bloqueos, candados |

**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** | La Ciberseguridad | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración (voz en off)** | **Texto** |
| **1** | Transición de imágenes con equipos de cómputo que muestren bloqueos o candados  **Protección de la información**  Suscribir, Registro, Software  Imágenes con dispositivos digitales en los que se visualice solicitud de acceso de contraseñas | NA | Es importante recordar que la ciberseguridad, consiste en la protección y confidencialidad de los sistemas e información. El manejo de grandes volúmenes de datos trae consigo un alto grado de responsabilidad y algunos riesgos. | Ciberseguridad para proteger la información |
| **2** | Recrear un *hacker* robando información  ***Hacker***  La seguridad de la red y los delitos contra la privacidad. Medios mixtos  Figura de *Hacker* robando información | NA | Primero, porque la información no es propiedad de la empresa que gestiona los datos sino de la persona directamente implicada, y segundo porque la información mal utilizada puede ser robada, borrada o alterada, afectando la disponibilidad, veracidad y fidelidad, que pondría en alto riesgo a los propietarios de esa información. | Cuidar la Información privada y confidencial  Evitar Robo de información |
| **3** | El mismo robo pero que se visualice que roban datos personales o información de  clientes o empresa.  **Robo de información**  Escándalo de phishing, ataque hacker a ilustración vectorial de smartphones  Un *hacker* robando información personal o documentos | NA | Por ejemplo, si la información es etiquetada como confidencial por una empresa y ésta llegara a manos de su competidor, quedarían expuestos todos los registros de clientes, estrategias comerciales, estados financieros, datos de accesos a portales bancarios, lo que causaría pérdidas de negocios, de clientes y demandas por exponer información confidencial, incluso hasta el cierre de la compañía, en general graves consecuencias. | Peligros al exponer la información |
| **4** | Una persona o superhéroe que cuida la información y es la ciberseguridad  **Ciberprotector**    Imagen de personas disfrazado de héroe con computadores y documentos, candados | NA | Ahora bien, dentro de ese vínculo se busca garantizar un correcto proceso para la protección de los datos y sistemas de información, incluso antes de la materialización de los riesgos, se puede lograr usando *hardware* y ***software*** que garantice la privacidad como un factor relevante y un modo de operación predeterminado para las organizaciones, en el que antes se puedan adoptar medidas preventivas de diversa naturaleza que eviten fallas de seguridad, vulneración en los derechos de privacidad, confidencialidad, y el uso indebido del tratamiento de datos personales. | *Hardware y software* que garantice la privacidad |
|  | **Lista de objetivos financieros**  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de planificación y gestión del tiempo - objetivos  Imágenes asociadas a ganancias económicas, también listas de cumplimiento |  | La dirección estratégica de la empresa debe cumplir unos objetivos financieros y estratégicos.  Algunos ejemplos de **objetivos financieros** son:  -El aumento en la producción en menor tiempo: El personal de la organización es fundamental para lograr este objetivo, este personal debe estar motivado y en constante preparación.  -Contratar más personal que permita la ejecución de mayor número de proyectos, aumentando las ganancias: La infraestructura física debe ser ampliada para garantizar el cumplimiento de este objetivo.  -Fortalecer la Imagen corporativa que genere una mayor demanda de clientes: Esto conlleva varios componentes a nivel tecnológico, operacional y de servicio al cliente. Se debe mitigar la pérdida de información confidencial con políticas de seguridad enfocadas a una mejora continua de los procesos por parte de todos los colaboradores. | Objetivos Financieros:  \_ El aumento en la producción en menor tiempo  -Contratar personal suficiente  \_ Fortalecer la Imagen corporativa |
|  | **Estrategias**  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de los empresarios suben escaleras, sosteniendo piezas de rompecabezas para lograr objetivos - objetivos  Personas trabajando en equipo |  | **Objetivos Estratégicos:**  -Estar preparado ante contingencias como desastres naturales: Sistema de BackUps con medios extraíbles móviles.  -Seguridad Física: La seguridad perimetral de los activos críticos de la organización debe estar garantizada. Los sistemas biométricos para control de entrada y sistema de sensores y alarmas para detectar intrusos no autorizados.  -Seguridad Lógica: Deben implementarse controles lógicos para salvaguardar los activos críticos a nivel de *software*. Se debe implementar una Política de contraseñas seguras, Firewall y sistema de detección de intrusos.  -Toma de conciencia: El personal de la organización debe ser consciente de la importancia de seguir los lineamientos del sistema de gestión para la seguridad de la información. Esto se logra realizando capacitaciones periódicas al personal sobre las políticas de seguridad que se deben cumplir para garantizar la integridad, disponibilidad e integridad de los activos informáticos. | Objetivos Estratégicos:  - Estar preparado ante contingencias  - Seguridad Física  - Seguridad Lógica  - Toma de conciencia |
| **Nombre del archivo** | **233103\_CF05\_v1.mp3** | | | |

**DESARROLLO DE CONTENIDO**

**1.** **Generalidades de la ciberseguridad**

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto |
| Para iniciar con el estudio de este componente formativo, es importante reconocer los aspectos relevantes que enmarcan la ciberseguridad en el entorno empresarial. Se abordarán los elementos asociados a la normatividad, las funciones y perfiles del personal encargado de la seguridad digital, los procesos de gestión, reportes de incidentes y documentación respectiva; es necesario reconocer las medidas que debe una empresa adoptar en temas de ciberseguridad. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo de recurso** | Carrusel de tarjetas | | |
| **Introducción** | Es así como se presentan los objetivos asociados y la medida en que se deben adoptar, para consolidar que la ciberseguridad es el comienzo hacía la implementación de un sistema de seguridad digital y algunas de estas medias son: | | |
| **Cod.Imagen:** 233103\_CF5\_i008 | | | |
| i) Evitar los accesos no autorizados a los equipos y a la información. | | **Accesos no autorizados**  Mobile phone unauthorized access prevention, login password verification, data protection, vector isometric illustration  Imágenes que involucren dispositivos electrónicos y personas impidiendo el acceso |
| ii) Evitar la manipulación de los equipos y de la información por medio de terceros no autorizados. | | **No tocar**  Handwriting text writing Restricted Access. Conceptual photo A class of service in which users may be denied access  Una imagen en la que se indique que no se puede tocar un PC, celular o un dispositivos, o que indique que tiene acceso restringido |
| iii) Evitar la destrucción de la información. | | **No destruir la información**  PCのハードディスクの破壊イメージ  Imágenes en las que se esté atentando contra dispositivos electrónicos, o medios digitales. |
| iv) Evitar los usos indebidos de la información. | | **Prohibido**  Man using laptop and icons with offensive messages, closeup. Cyber bulling concept  Personas con equipos de cómputo en los que aparezcan alertas sobre NO PERMITIDO |
| v) Evitar el suministro de información a personas no autorizadas o claves de accesos a equipos que tengan el control de la red. | | **Claves y contraseñas confidenciales**  Access denied sign on laptop screen. Hand from device showing user does not have permission to file, system refuses password and entry to computer data, error with red signal. Vector illustration  Pantallas de PC en las que aparezcan mensajes solicitando autenticación o alertando de acceso denegado |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| En el desarrollo de las tecnologías, *software* y algoritmo del sistema de información se presentan unos riesgos que influyen sobre la planificación en la protección de la red y el tratamiento de los datos o sistemas de información, por ejemplo: dentro de la operación de algoritmos se pueden producir sesgos humanos o fallas técnicas en la implementación, sólo a través de estas medidas se podrán controlar y evaluar los riesgos desde la normativa para que no afecten la seguridad de la información y no se vulneren los derechos de los titulares de los datos.  **Medidas preventivas**  Bypass Captcha, Anti Captcha, Solving service, AI. Robot clicking on captcha - I am not a robot. Cartoon modern flat vector illustration for banner, website design, landing page.  Personas con equipos de cómputo tratando de acceder sin lograrlo porque tiene sistema de seguridad. | |

**Normativa**

|  |  |
| --- | --- |
| **Tipo de recurso** | **Cajón de texto** |
| En Colombia, las normas asociadas a la explotación de datos, protección y denuncia surgen por diferentes necesidades y objetivos, que requieren un alcance que no está directamente relacionado con la aplicabilidad de *Big Data*, sin embargo, es importante conocer que existen normas, decretos, leyes que respaldan y protegen la explotación de datos. | |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| La normativa es parte fundamental en el manejo de datos y esta se debe seguir tal cual está estipulada. En el CONPES 3920 - Marco de la Política Nacional de Explotación de datos (2018), el desarrollo de marcos normativos y políticas públicas se adaptan a todos los avances tecnológicos y responden de manera pertinente a los requerimientos de la sociedad; es por ello, que se ha convertido en una necesidad imperiosa el aprovechamiento óptimo y eficiente de los datos, que generan beneficios para todas las entidades cumpliendo con los requisitos de transparencia, divulgación de información y toma de decisiones.  Del mismo modo, en el CONPES 3995 (2022) describe la política nacional cuyo objetivo es establecer medidas en búsqueda de ampliar la confianza digital, mejorando la seguridad digital de manera que Colombia se define como sociedad incluyente, además de competitiva en el mundo digital.  **Normativa**  Businessman touching the icon of the balance of justice. Concept of legal advice, law and defense.  Imágenes que asocian símbolos de normas y leyes, documentos | |

|  |  |  |
| --- | --- | --- |
| **Tipo de recurso** | Tarjetas Avatar | |
| **Introducción** | El aprovechamiento y recolección de datos está regido por diferentes normas y decretos que es importante tener en cuenta dentro del marco jurídico: | |
| Constitución Política de Colombia 1991: artículo 15 mediante el cual se establece el derecho que tienen las personas a conocer, actualizar y ratificar la información personal. | | Identification card outline icon isolated on background. Identification card , Identification card logo,. Editable stroke. Vector illustration. Eps 10 Identification card |
| Ley 1266 de 2008: por medio de la cual se dictan las disposiciones generales de habeas data. | | Businessman stealing a user's personal data |
| Ley 1273 de 2009: modifica el código penal y crea como bien jurídico tutelado la protección de la información y de los datos. | | Cyber security network. Padlock icon and internet technology networking. Businessman protecting data personal information on tablet and virtual interface. Data protection privacy concept. GDPR. EU. |
| Ley 1581 de 2012: principios y disposiciones que definen los derechos sobre los datos personales y denuncia de las violaciones de seguridad. | | Man touching a personal data security concept |
| Decreto 1377 de 2012: reglamentó aspectos relacionados con la titularidad del uso de la información para el tratamiento de sus datos personales. | | The Personal Data Protection Act PDPA sign on the screen and gavel. |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto |
| **Normatividad y marco legal**  Para ampliar la información respecto a la normatividad y marco jurídico asociado a la recolección de datos puede acceder a los documentos anexos.  **Crear botón o enlace**  **Ver aquí Anexos: Normatividad y marco legal** | |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto |
| Es importante que las entidades públicas consideren el diseño e implementación de una arquitectura de almacenamiento de datos, que respalde la confidencialidad, integridad y disponibilidad de éstos, debido a la cantidad de datos que recolectan y/o generan, es así que requieren la implementación de una adecuada gestión de la información para asegurar la protección, almacenamiento y acceso de los datos.  Negocio contenido en línea .Web diseño estructura y diseño. - arte vectorial de Internet libre de derechos | |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto |
| Teniendo en cuenta la importancia de una arquitectura de almacenamiento de datos, hay una normativa legal en la empresas que deben establecer unas políticas de usuario que permitan el desarrollo de un Sistema de Gestión de Seguridad de la Información, que debe iniciar con la documentación de procesos y conociendo cómo opera la organización, también revisar el manual de funciones de cada empleado cómo paso fundamental para aplicar el ciclo Planear-Hacer-Verificar-Actuar PHVA, y en la acción, para planear es necesario conocer los procesos digitales críticos en la organización, que luego detalladamente se deben analizar para implementar controles que puedan proteger los procesos implementados ante amenazas cibernéticas.  Mujeres empresarias discutiendo sobre notas adhesivas - Foto de stock de Lista de tareas libre de derechos | |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| El ciclo PHVA, cobra gran importancia en los procesos de ciberseguridad y entender cada una de las fases, por ejemplo en planear es posible detectar las amenazas internas, que parecieran ser externas porque vienen del internet, y que en realidad no son a causa de un ser humano con intenciones maliciosas, sino de los mismos empleados que al no estar capacitados descargan programas que vienen con virus tipo troyanos o sin intención maliciosa que puede mover un directorio o archivo, también se deben revisar las políticas que tengan contempladas el departamento de Tecnologías de la Información (TI) de la organización. | |

|  |  |
| --- | --- |
| **Tipo de recurso** | Tarjetas Conectadas |
| **Introducción** | La importancia de bajar las amenazas es indispensable, así como existen algunas recomendaciones: |
| fingerprint authorization access concept, personal data information security | |
| **Cod.Imagen:** 233103\_CF5\_i019 | **Proteger los equipos:** mantener actualizado el sistema operativo y el antivirus es fundamental porque corrigen agujeros de seguridad. |
| **Cod.Imagen:** 233103\_CF5\_i020 | **Contraseñas fuertes:** números consecutivos, fechas de cumpleaños, nombre de nuestros hijos, equipo de fútbol favorito, son ejemplos de contraseñas poco seguras. Se recomienda usar contraseñas cambiando letras mayúsculas y minúsculas, números y caracteres especiales, ejemplo: AbgDho-9823\*#. |
| **Cod.Imagen:** 233103\_CF5\_i021 | **Utilizar protocolos de seguridad:** clave de acceso al computador o servidor, generar cuentas de usuario con contraseñas para equipos compartidos, bloquear el equipo cuando no se esté en frente de él, son buenos protocolos de seguridad. |
| **Cod.Imagen:** 233103\_CF5\_i022 | **Evitar dar datos personales:** mantener la cautela y desconfianza en redes sociales, no compartir datos con contactos o perfiles sospechosos, no aceptar sugerencias o amigos no conocidos. |
| **Cod.Imagen:** 233103\_CF5\_i023 | **No descargar contenido pirata:** descargar música, libros, películas, videos, *software* de sitios recomendables, siempre tener cuidado de páginas poco conocidas. |
| LIVE STREAMING Backup Download Computing Digital Data transferring , STREAMING Download  **Cod.Imagen:** 233103\_CF5\_i024 | **Realizar una copia de seguridad:** es importante evitar depender de una sola fuente de información, es recomendable tener copia de respaldo de nuestro equipo en algún disco duro externo o en la nube. |

**Perfil profesional y funciones**

|  |
| --- |
| **Cuadro de texto** |
| Las personas que hacen parte de la gestión de la seguridad, también se encuentran establecidas bajo una normativa de seguridad de la información ISO/IEC 27001 y la ISO/IEC 27002, a través de la generación de instrumentos e informes para el proceso de auditoría de los SGSI, es así que existen dos perfiles de profesionales para la implementación de la normatividad: director de seguridad y profesional de seguridad. A continuación, se describe cada perfil, según las acciones y funciones. |

**Profesionales de seguridad informática**

|  |  |
| --- | --- |
| **Tipo de recurso** | Acordeón tipo 1 |
| **Introducción** | Se inicia con el perfil de **director de seguridad** quien lidera el proceso, reconozcamos las funciones propias de su cargo las cuales son: |
| equipo de seguridad de red de protección y seguro su concepto de datos. el crimen digital de un hacker anónimo - personal de seguridad informatica fotografías e imágenes de stock | |
| **Identificación de procesos y activos**  Junto con cada uno de los departamentos de la organización se identifican los procesos y activos, para determinar cuáles son los de nivel crítico, que al darse un ataque podrían afectar la operación e incluso la continuidad del negocio. | |
| **Identificar Amenazas**  Luego de realizar el inventario de activos, se procede a identificar cada una de las amenazas a los que estos están expuestos. Para esto se pueden aplicar metodológicas establecidas como Magerit, octave, cobit, etc. | |
| **Establecer controles de seguridad**  Se definen medidas de seguridad para implementar en la organización y mitigar el riesgo de que las amenazas se materialicen y se genere un incidente informático. | |
| **Priorización en la implementación de controles**  Con base en los objetivos estratégicos, se determina cuáles son las primeras medidas para implementar, categorizando según el tiempo en corto, mediano y largo plazo, ya que no se pueden implementar todas las medidas de inmediato. | |
| **Revisión posterior**  Al terminar la ejecución del plan de seguridad se debe hacer un análisis total de procesos y activos, para determinar las novedades. | |

|  |  |
| --- | --- |
| **Tipo de recurso** | Acordeón tipo 2 |
| **Introducción** | Los otros perfiles están asociados a los profesionales de seguridad informática, de acuerdo a las funciones se asigna un nombre específico, a continuación, la descripción de algunos: |
| concepto de seguridad cibernética. protección de la red. - personal de seguridad informatica fotografías e imágenes de stock | |
| **Administrador de seguridad de red**  Encargado de la seguridad del hardware y *software* de toda la red, elementos como *routers, switches, firewalls, IDS, IPS, DNS etc*. | |
| **Jefe de sistemas -CIO**  Principal responsable del área TI , encargado de idear las estrategias tecnológicas de la organización. | |
| **Administrador de seguridad perimetral**  Entre sus funciones principales se encuentra manejar los elementos que protegen a los activos críticos de acceso físico no autorizado. Esto a través de elementos como sensores de movimiento, alarmas, dispositivos biométricos, entre otros. | |
| **Director de la seguridad de información-CISO**  Su perfil es a nivel ejecutivo alineando la seguridad de la información con los objetivos estratégicos del negocio. Entre sus funciones están implementar las políticas de seguridad y supervisar la respuesta ante incidentes informáticos. | |
| **Arquitecto de seguridad**  Aplicar un método para describir la estructura y los procesos de seguridad de la organización, diseñar la arquitectura de seguridad informática, análisis de requerimientos relacionados con la seguridad. | |
| **Jefe de seguridad - CSO**  Responsable de la seguridad corporativa, se diferencia del CISO porque está más centrado en la seguridad de la información. Mientras que el CSO gestiona los planes de continuidad de negocio, riesgos y las normativas vigentes. | |
| **Consultor de seguridad y *hacking* ético**  Puede ser interno o externo, teniendo grandes conocimientos en seguridad ofensiva y se encarga de realizar test de penetración y pruebas en general para determinar el estado de seguridad informática de los ciberactivos críticos, detectando amenazas y vulnerabilidades que puedan materializarse con el ataque de delincuentes informáticos. | |
| **Auditor de seguridad de la información**  Personal con amplios conocimientos en normativas vigentes respecto a la seguridad de la información como por ejemplo ISO27001:2013, el cual realiza una evaluación sobre el cumplimiento del sistema de gestión de seguridad de la información en la organización, levantando no conformidades frente a los objetivos trazados que se estén incumpliendo y sugiriendo la manera de que estos se lleven a cabo de forma exitosa. | |

**Proceso para la gestión de seguridad digital**

|  |
| --- |
| **Cuadro de texto** |
| Las buenas prácticas y el concepto de Gestión en Sistemas de Seguridad Informática y de la Información (SGSI) son indispensables para implementar un proceso de gestión de seguridad digital siendo necesario la identificación de las fuentes de riesgos, seleccionar las herramientas para la valoración del riesgo, clasificar el impacto de las amenazas para realizar la gestión que permita proteger la empresa ante las posibles consecuencias. |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| La ciberseguridad ha cobrado importancia en los últimos años; en el tema de calidad de la información se han estandarizado los procesos y en la seguridad informática se han implementado algunos controles y planes. Con la llegada de la norma ISO 27000 aparecen los conceptos y buenas prácticas de Gestión en Sistemas de Seguridad Informática y de la Información (SGSI), que gracias a las nuevas tecnologías y los sistemas de información se alinean en estándares que hasta el momento habían sido aplicados al análisis de riesgos informáticos y que posteriormente han sido usados para la gestión de riesgos de ciberseguridad.  ISO27001 banner web icon vector illustration concept for  information security management system (ISMS) with an icon of technology, standards, control, security, certification, and verified  **Cod.Imagen:** 233103\_CF5\_i027  <https://t4.ftcdn.net/jpg/04/91/11/61/240_F_491116138_CUWSSTDZkUDa1wgBmRjEnQ53XZlGMe1n.jpg>  El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información y de los equipos que operan en la red, buscando asegurar los activos de información que son el valor más importante en una organización; minimizando a la vez los riesgos de seguridad de la información: Integridad, confidencialidad y disponibilidad. | |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| La valoración del riesgo asegura que el SGSI logre los efectos previstos, y con las mismas herramientas se puede prevenir o reducir efectos indeseados, logrando la mejora progresiva, integrando e implementando acciones en los procesos del sistema de gestión de la seguridad de la información. Existen empresas en el mundo que ofrecen una gran cantidad de herramientas para la valoración del riesgo como:   * spiraPlan de inflectra * Rastreados a 1 * IsoMetriz * Entre otras   Computer security | |

|  |  |  |
| --- | --- | --- |
| **Tipo de recurso** | Slider Presentación | |
| **Introducción** | En la identificación de riesgos se debe recordar que la inseguridad se enuncia en procesos de la composición de los resultados de un suceso y la probabilidad de ocurrencia asociada. | |
| **Las fuentes de riesgos pueden ser:**   * Legales. * Comportamiento humano (interno y externo). * Comerciales. * Economía y mercado. * Circunstancias políticas * Tecnología. * Eventos naturales. * Organizacionales. | | Data analysis concept. Teamwork of business analysts on holographic charts and diagrams of sales management statistics and operational reports, key performance indicators. Flat vector illustration |
| En la gestión del riesgo de ciberseguridad se debe proteger la empresa ante las posibles consecuencias, como:   * Pérdidas de confidencialidad. * Integridad. * Disponibilidad. * No-repudio. * Autenticidad. * Confiablidad de los activos. * Incumplimiento de la legislación. * Pérdidas financieras. * Impacto de orden público. * Impacto de orden internacional. | | Isometric Internet And Personal Data Hacker Attack Concept. Website Landing Page. The Hacker at The Computer Trying To Hack Security. Credit Card, Bank Account Hacking. Web Page Vector Illustration |
| Es importante el impacto luego de conocer el estado real de seguridad de un activo antes y después de materializar las amenazas. En un SGSI, al concretarse una amenaza, el activo cambia de estado, es decir, antes de producirse la amenaza se tiene un valor al activo y después que se efectúe la amenaza se tiene la diferencia entre el estado anterior y el posterior a la amenaza. | | isometric vector image on a dark background, a transparent shield covering the laptop from virus attacks, protection of digital data |
| Clasificación según el tipo de impacto como:   * Extremo. * Importante. * Moderado. * Menor. * Incidental.   Cada clasificación se puede crear o diseñar dependiendo del tamaño de la organización y el valor podría darse en un rango de 0 a 5. | | Hacking concept. Personal information and credit card detail. |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| **El SGSI y la gestión del riesgo**  Guía Icontec internacional educación  A continuación, podrá identificar las diferentes estrategias de mejora continua a través del ciclo PHVA.    **Cod.Imagen:** 233103\_CF5\_i033  El SGSI y la gestión del riesgo-Guía Icontec internacional de educación. Fuente: Guía de Gestión de riesgos de seguridad de la información, 2021. Recuperado de <https://www.icontec.org>  ara el diseñador, por favor configurar el gráfico para que el aprendiz interactúa con el ciclo, se puede hacer con puntos calientes y que a manera de gif se mueva en ciclo.  P  -Establecer el contexto  -Evaluar el riesgo  -Planificar el tratamiento  -Aceptación  H  -Implementar el plan de tratamiento del riesgo  V  -Monitorear y revisar continuamente los riesgos  A  -Mantener y mejorar el proceso de gestión del riesgo | |

**Documentación y reporte de procesos**

|  |
| --- |
| **Cuadro de texto** |
| Para iniciar con el estudio de este tema, se realiza un recorrido en línea de tiempo sobre la evolución de la tecnología para luego describir las partes que componen el documento con la información y los reportes de procesos. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tipo de recurso** | Video spot animado | | | |
| **NOTA** | **La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente** | | | |
| **Título** | **Documentación y reporte de procesos** | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración (voz en off)** | **Texto** |
| **1** | 1.Que aparezcan imágenes asociadas a las revoluciones industriales en un orden, una después de la otra y puede ir formando un círculo  **Revolución industrial**  Industry 4.0 technology concept - Smart factory for fourth industrial revolution with icon graphic showing automation system by using robots and automated machinery controlled via internet network .  2. Personas trabajando en casa y desde otros lugares  **Teletrabajo**  Asian business man stay with family and work remotely at home video conference remote call to corporate group. Meeting online,videocall, group discuss online concept.  **Trabajando desde cualquier lugar del mundo**  Skilled female digital nomad working remotely creating trip guide to high mountains for share to followers in social networks connected to 4g internet, skilled freelancer typing text on laptop | Música de fondo | En la era de la cuarta revolución industrial, las organizaciones migraron al teletrabajo y home office, nacieron conceptos como nómadas digitales, donde un trabajador desde cualquier parte del mundo puede cumplir con sus obligaciones y funciones contractuales, por lo que es fundamental que la organización se blinde ante la fuga de información, y a posibles ataques cibernéticos. | 1.Cuarta Revolución industrial  2. teletrabajo, home office, nómadas digitales |
| **2** | Un carrusel de imágenes correspondiente a cada texto que aparezcan una después de la otra, asociados a peligros en la red, computadores con bloqueos o alertas  1.  **Riesgos cibernéticos**  cybersecurity concept, user privacy security and encryption, secure internet access Future technology and cybernetics, screen padlock.  2.  **Políticas de seguridad**  Normative – Statistics/Business. Laptop in the office with term on the display. Finance/Economics.  3.  **Sistemas de seguridad**  Virtual screen icons Document Management System (DMS) Online document file data software for efficient archiving lead to successful business process for company.  Un conjunto de iconos o imágenes asociadas a la seguridad de la información, pc, antivirus, | Música de fondo | Dentro de las generalidades y aplicaciones de la ciberseguridad está la capacidad de identificar las formas en que se puede dar el tratamiento de riesgos, los tipos de control y la integración con las políticas y procedimientos para la estructuración de SGSI. De este modo, se deben establecer controles y planear el punto de partida de las mejoras a implementar. Con un SGSI, la empresa conoce los riesgos a los que está sometida su red e información, y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente. | 1.Tratamiento de riesgos  2.Políticas de seguridad  3.Gestión en Sistemas de Seguridad Informática y de la Información (SGSI) |
| **3** | Imagen en la que aparezcan personas con equipos de cómputo, ojalá ingresando claves o simulando bloqueos o candados  **Riesgos**  Multiethnic cyber security team developing software algorithm for information processing and network optimization. Informational agency multiracial tech enginners programming application while using | Música de fondo | Con un SGSI, la empresa conoce los riesgos a los que está sometida su red e información, y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente. | Todos en la empresa deben conocer los riesgos |
| **4** | Personas con documentación digital y reportes  **Informes y Reportes**  Business Documents, Auditor businesswoman checking searching document legal prepare paperwork or report for analysis TAX time,accountant Documents data contract partner deal in workplace office | Música de fondo | La documentación y los reportes de procesos son un documento que describe el progreso de una investigación o labor realizada, que está conformado por la presentación sistemática, cronológica y con la información suficiente para que el lector con capacidad y conocimiento de los hallazgos reportados, pueda evaluar y proponer alternativas de solución o implementación con el fin de evitar situaciones indeseables. Éste, debe estar conformado como mínimo por: parte inicial, cuerpo, anexo y parte final. | Documentación y Reportes |
| **Nombre del archivo** | **233103\_CF05\_v2.mp3** | | | |

|  |  |  |
| --- | --- | --- |
| **Tipo de recurso** | Infografía interactiva Punto caliente | |
| **Texto introductorio** | El documento con la información y los reportes de procesos se divide de la siguiente manera: | |
|  | | |
| **Código de la imagen** | **Cod.Imagen:** 233103\_CF5\_i042 | |
| **Punto caliente 1** | **Parte Inicial**   * Portada. * Resumen. * Índice. * Glosario de signos, símbolos, unidades, abreviaturas, términos técnicos. * Prefacio | Si es posible modificar el icono 1 por uno similar en el que se pueda leer la palabra índice |
| **Punto caliente 2** | **Cuerpo del informe**   * Introducción. * Núcleo del informe con tablas, imágenes y demás material complementarios. * Conclusiones y recomendaciones. * Agradecimientos. * Listas de referencia. | Un icono similar al del punto 2 y que se visualice una tabla y un gráfico |
| **Punto caliente 3** | **Anexos**   * Los anexos se consideran separadamente de la parte final, porque, aunque en muchas ocasiones no se requiere, en otras, forman parte esencial y complemento de información de algunos informes. Se usan para presentar material que complementa el texto, éstos pueden ser: tablas, imágenes, material especial, bibliografía, descripción de equipos, *software*, etc. | Un icono similar al del punto 3 con el clip que indica anexo o adjunto |
| **Punto caliente 4** | **Parte final**   * Hojas de datos del documento. * Lista de distribución y disponibilidad. * Cubierta posterior, si se requiere.   . | Un icono similar al del punto 4 con listas de texto |

**2.** **Aplicación de ciberseguridad**

|  |
| --- |
| **Cuadro de texto** |
| En la implementación de la ciberseguridad en la organización son necesarias herramientas de *hardware y software*, además de cumplir con las directrices de las políticas y normas establecidas para efectos de seguridad de la información, en pro de la accesibilidad y perdurabilidad de la información digital. Para el desarrollo de este tema se presenta un ejemplo de *software* malicioso, una lista de recomendaciones de cómo protegerse contra el malware y cómo realizar el registro de eventos e incidentes. |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| De acuerdo a los nuevos requerimientos de la administración pública derivados de la Ley de Transparencia, Ley de Protección de Datos y Ley General de Archivos, nace la necesidad de crear una directriz que permita a las entidades garantizar la accesibilidad y perdurabilidad de la información digital. De este modo, se genera el uso de diversos formatos, medios, equipos de almacenamiento digital y surgen nuevas formas de buscar y analizar la información.  En la actualidad, la mayor parte de la información reside en servidores, redes de información y almacenamientos como nube, discos extraíbles, Backups, enmarcados dentro de lo que se conoce como sistemas de información. Estos sistemas de información están sujetos a vulnerabilidades, ataques informáticos, riesgos e inseguridades dentro de la propia organización como desde fuera.  Black external hard disk connecting to a laptop on a blue background. | |

|  |  |  |
| --- | --- | --- |
| **Tipo de recurso** | Slider Presentación | |
| **Introducción** | Tal como se informó, se presentará el ejemplo de un *software* malicioso, con el fin de contextualizar lo que podría pasar. | |
| Un ejemplo claro es el *software* malicioso más conocido como “malware”, éste es un *software* diseñado por un tercero con la única finalidad de obtener acceso no autorizado a un equipo para robar información o simplemente dañarlo. En la actualidad existen diferentes tipos de malware: spyware, registradores de pulsaciones, virus, gusanos, etc. | | Concept of cyber crime, hand using laptop and show malware screen that comes with email, hack password and personal data. |
| La creación de malware cada vez aumenta más, esto se debe a que se crean nuevos tipos de malware a diario por el uso activo de los usuarios de las redes que son vulnerables a los ataques cibernéticos. Inicialmente, el malware se creó a manera de entretenimiento, pero luego evolucionó al vandalismo y destrucción de equipos. Hoy en día, la mayoría de malware son creados para ganar dinero mediante extorsión (ransomware), publicidad forzada (publicidad no deseada), difusión de spam o pornografía por correo electrónico (equipos zombis), robo de información confidencial (spyware). | | Resumen Advertencia de un programa de malware detectado - Foto de stock de Spyware libre de derechos |
| Diversos factores pueden hacer que un equipo sea más vulnerable a ataques de malware, como equipos de trabajo sin la licencia de un antivirus confiable, desactualización de base de datos de antivirus y sistemas operativos, defectos en el diseño del sistema operativo, equipos conectados a una red que estén ejecutando el mismo sistema operativo, etc. | | Intrenet security problem |

|  |  |
| --- | --- |
| **Tipo de recurso** | Infografía estática |
| **Texto introductorio** | En el gráfico se presentan algunas recomendaciones sobre cómo protegerse contra el *malware*. |
| * Ser cautelosos. * No confiar en correos de remitentes no conocidos. * Ejecutar archivos adjuntos de correos electrónicos no deseados. * Mantener actualizado el antivirus. * No navegar por páginas poco confiables. * Descargar los programas que serán instalados en el computador de sitios confiables. * Mantener actualizadas las bases de datos y las mejoras del sistema operativo.   **Modificar los iconos por otros más representativos o imágenes.** | |
| **Código de la imagen** | **Cod.Imagen:** 233103\_CF5\_i047 |

**Herramientas de *hardware* y *software***

|  |
| --- |
| **Cuadro de texto** |
| Para prevenir estos ataques informáticos se hace necesario el uso de una poderosa infraestructura de TI que ayude a detectar y frenar amenazas. En este item se describen algunos elementos que son parte de la infraestructura de TI para detectar y frenar amenaza. |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| La seguridad informática y la seguridad de la información están encargadas de proteger los datos contra robo de información, acceso no autorizado, obstaculización al sistema informático, manipulación y/o eliminación de datos. Cuando se habla de procesos empresariales impulsados en la transformación digital con tecnología de punta, se entiende que están expuestos a diferentes vulnerabilidades, amenazas y ataques informáticos dirigidos a la seguridad y la privacidad de la información. Mediante la norma ISO 27001, la implementación del SGSI sigue el modelo Planificar – Hacer – Verificar – Actuar, para la mejora continua de los procesos.  Software hardware concept  Sin embargo, la seguridad para las empresas es un tema cada vez más crítico y de preocupación constante, debido a que los ciberataques pueden ser tan catastróficos como un robo, explosión o un incendio.. | |

|  |  |  |
| --- | --- | --- |
| **Tipo de recurso** | Slider pasos | |
| **Introducción** | Algunos elementos que son parte de la infraestructura de TI para detectar y frenar amenazas son: | |
| **Slide 1** | ***Software* antivirus**  En cualquier caso, todos los computadores que estén conectados a una red interna o internet, deben contar con un antivirus gratuito o pago pero que sea confiable. Estos programas permiten contar con medidas de protección efectivas cuando el equipo se encuentre expuesto a *software* malicioso o cualquier otro tipo de malware; Estos programas ofrecen la oportunidad de eliminarlo por completo o poner en estado de cuarentena.  *Kaspersky, Avast, Nod32, McAfee,* son algunas de las posibilidades que se pueden encontrar en el mercado actual, lo más importante es que cualquier solución de antivirus en la que el usuario quiera confiar, debe tener la certeza que se adapte a las necesidades de seguridad y cuentan con actualizaciones constantes, debido a que los malware están en continua evolución. | Hombre de negocios maduro mirando una pantalla de inicio de sesión de seguridad antivirus en una computadora. - Foto de stock de Software antivirus libre de derechos |
| **Slide 2** | ***Firewall* perimetral de red**  Como su nombre lo indica, hace la función de una pared de bloqueo. Es un sistema cuya función es prevenir y proteger la privada de ataques de otras redes. Su funcionamiento es sencillo: escanea los paquetes de red, permitiéndoles o bloqueándolos según las reglas definidas por un administrador. | Firewall de computadoras - Foto de stock de Servidor de seguridad libre de derechos |
| **Slide 3** | **Servidor proxy**  Un proxy es un es un servidor, puede ser un programa o dispositivo físico, que actúa de intermediario entre conexiones del navegador e internet, filtrando todos los paquetes entre ambos. Así mismo, establece un sistema de autentificación, que limita el acceso a la red externa, por lo cual, se puede generar los registros sobre sitios, visitas, y demás datos de navegación. | Iconos lineales del servidor proxy establecidos - arte vectorial de Servidor de red libre de derechos |
| **Slide 4** | **Cifrado de punto final o *end point disk encryption***  Contiene el proceso para codificación de datos, de tal forma que no puedan ser leídos por agentes externos que no cuenten con la clave para decodificarlos. Es decir, genera protección de los sistemas operativos ante cualquier instalación o ejecución de agentes corruptos, logrando bloquear todos los archivos almacenados en el servidor, o cualquier otro punto final. | Fondo vectorial de falla de pantalla de error de código de programa - arte vectorial de Codificar libre de derechos |
| **Slide 5** | **Escáner de vulnerabilidades**  Es un *software* que detecta puntos frágiles en los sistemas informáticos de las empresas, con el objetivo de analizarlos y gestionarlos, dando respuesta oportuna a cualquier evento desafortunado. Con este sistema se puede controlar las amenazas y consecuencias en los activos digitales, además de generar alertas en tiempo real, ayudando a solucionar incidentes sin que se llegue a comprometer el normal desarrollo de los procesos en las empresas. | Concepto de prueba de seguridad de aplicaciones - AST - Ilustración 3D - Ilustración de stock de Tecnología libre de derechos |

**Eventos e incidentes**

|  |
| --- |
| **Cuadro de texto** |
| Para finalizar el tema de estudio en este componente, es necesario definir los eventos e incidentes que permiten documentar los diferentes casos asociados a riesgos, amenazas detectadas o daños causados en el sistema de información de la empresa, cómo se describe a continuación. |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| Las normas y los sistemas de gestión relacionan la “gestión de incidencias” como medida a las interrupciones que se puedan presentar en los procesos de negocio; los términos más utilizados son **los eventos y los incidentes**.  Por evento se entiende como un cambio que no genera resultados negativos, es decir, el evento no trae implicaciones negativas, de este modo, puede ser usado como una expresión neutral, por el contrario, el incidente si representa resultados negativos, y pueden verse como las interrupciones o desmejoramiento en la calidad de los servicios prestados a los usuarios. Los incidentes deben atenderse mediante la estructura de gestión de incidencias.  Una imagen tipo Evento  el líder del proyecto y el director ejecutivo discuten los datos mostrados en un portátil. en la pantalla grande de fondo que muestra infografías de infraestructura, gráficos, análisis del sistema. sala de control de telecomunicaciones - ciberseguridad fotografías e imágenes de stock  Una imagen tipo Incidente  hacking y red ransomware concepto - ciberseguridad fotografías e imágenes de stock | |

|  |  |  |
| --- | --- | --- |
| **Tipo de recurso** | Carrusel de tarjetas | |
| **Introducción** | Según la norma ISO 27001 el incidente genera un impacto de las operaciones de la seguridad de la información, según el nivel de afectación se pueden clasificar los incidentes según el impacto generado como: | |
| Imagen general que ilustre el tema (opcional) | | |
| **Confidencial:** Reserva de la información. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de icono de documento confidencial, ilustración aislada lineal, vector de línea fina, signo de diseño web, símbolo de concepto de contorno con trazo editable sobre fondo blanco. - icono confidencial  **Cod.Imagen:** 233103\_CF5\_i056 |
| **Integridad:** Información completa sin alteraciones. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de diseño de iconos de línea de compatibilidad de productos - icono informacion incompleta  **Cod.Imagen:** 233103\_CF5\_i057 |
| **Disponibilidad:** Garantizar el acceso a las personas con los permisos o credenciales requeridas. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de las personas se registran en el conjunto en línea. registrarse o registrarse en la interfaz de usuario. los usuarios utilizan el inicio de sesión seguro y la contraseña. colección de registro en línea, registro, interfaz de usuario. ilustraciones vect - acceso al sistema  **Cod.Imagen:** 233103\_CF5\_i058 |

|  |
| --- |
| **Cuadro de texto** |
| Recuerde explorar los demás recursos que se encuentran disponibles en este componente formativo; para ello, diríjase al menú principal, donde encontrará la síntesis, una actividad didáctica para reforzar los conceptos estudiados, material complementario, entre otros. |

**SÍNTESIS**

El siguiente mapa integra los criterios y especificidades de los conocimientos expuestos en el presente componente formativo.

|  |  |
| --- | --- |
| **Tipo de recurso** | Síntesis |
| Técnico en Control de la Seguridad Digital  Síntesis: Ciberseguridad, Generalidades y aplicaciones | |
| **Introducción** | Como refuerzo se presenta a continuación la síntesis del componente formativo de una forma gráfica, así podrá repasar las diferentes temáticas tratadas en el componente. |
| CIBERSEGURIDAD  ISO 27001  *Hardware*  *Software*  Eventos e Incidentes  **ISO 27001** - Estándar para la seguridad de la información. Comprende normas y procesos para gestión de eventos e incidentes mediante *Hardware* y Software  ***Hardware*** - Equipos informáticos que gestionan de manera física el acceso a los sistemas digitales de la información  ***Software***- Programas informáticos que gestionan de manera digital el acceso a los sistemas de la información almacenados en el *Hardware*  **Eventos e incidentes** - Cambios o acceso no autorizado a los sistemas de información que pueden ocasionar daños o no disponibilidad de los servicios  **CIBERSEGURIDAD**  **ISO 27001** - Estándar para la seguridad de la información. Comprende normas y procesos para gestión de eventos e incidentes mediante *Hardware* y *Software*  **Hardware** - Equipos informáticos que gestionan de manera física el acceso a los  sistemas digitales de la información    ***Software***- Programas informáticos que gestionan de manera digital el acceso a  los sistemas de la información almacenados en el *Hardware*    **Eventos e incidentes** - Cambios o acceso no autorizado a los sistemas de información que pueden ocasionar daños o no disponibilidad de los servicios | |

|  |
| --- |
| **Cuadro de texto** |
| Recuerde explorar los demás recursos que se encuentran disponibles en este componente formativo, para ello diríjase al menú principal en donde encontrará la síntesis, una actividad didáctica, material complementario, entre otros. |

**ACTIVIDAD DIDÁCTICA**

Esta actividad le permitirá determinar el grado de apropiación de los contenidos del componente formativo.

De acuerdo con la definición planteada en la columna izquierda, arrastre cada término al lugar que considere correcto de la columna derecha.

|  |  |  |
| --- | --- | --- |
| **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. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de verificación de personalidad, acceso seguro a cuentas, protección de datos de privacidad, concepto vpn. sitio web, seguridad de datos o privacidad - ciberseguridad |
| Componentes físicos del computador, es decir, todo lo que se puede ver y tocar | | *Hardware* |
| Programa o dispositivo físico, que actúa de intermediario entre conexiones del navegador e internet, filtrando todos los paquetes entre ambos | | Proxy |
| Cambios entre letras mayúsculas y minúsculas, números y caracteres especiales, ejemplo: AbgDho-9823\*# | | Contraseñas fuertes |
| Probabilidad que un evento desafortunado ocurra y genere consecuencias a una persona, entidad o cosa | | Riesgo |
| Consiste en la protección y confidencialidad de sistemas e información | | Ciberseguridad |
| Todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos. (Sistemas operativos, aplicaciones, etc.) | | Software |

Retroalimentación General:

**Mensaje positivo >= 7/10** – FELICITACIONES – Tiene claro los conceptos básicos de las herramientas y buenas prácticas que garantizan la protección de los datos e infraestructura IT antes vulnerabilidades y riesgos, además, reconoce y comprende las diferentes normas, leyes y decretos fundamentales que debe implementar las instituciones en ciberseguridad.

**Mensaje negativo < 7/10** – Estimado aprendiz, es importante repasar nuevamente el contenido del componente formativo, los conceptos de herramientas y buenas prácticas, así como las normas, leyes y decretos en ciberseguridad no se ha comprendido en su totalidad.

**MATERIAL COMPLEMENTARIO**

|  |  |  |  |
| --- | --- | --- | --- |
| Tipo de recurso | Material complementario | | |
| Tema | Referencia APA del material | tipo | Enlace |
| Generalidades de la ciberseguridad | Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2016). *Gestión Del Riesgo: Orientación Para La Implementación De La NTC-ISO 31000 = Risk Management: Guidance for the Implementation of ISO 31000.* Icontec.  <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000012244> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000012244> |
| Generalidades de la ciberseguridad | Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2014). *Tecnología De La Información: Técnicas De Seguridad. Gestión De Incidentes De Seguridad De La Información.* ICONTEC. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/q6j6k0/sena_aleph000075887> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/q6j6k0/sena_aleph000075887> |
| Generalidades de la ciberseguridad | Razak, M. F. A., Nor Badrul Anuar, N. B., Salleh, R. & Ahmad, F. (2016). The Rise of “malware”: Bibliometric Analysis of Malware Study. *Journal of Network and Computer Applications 75*, p. 58-76.  <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_gale_infotracacademiconefile_A518245030> | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_gale_infotracacademiconefile_A518245030> |

**GLOSARIO**

|  |  |
| --- | --- |
| **Tipo de recurso** | Glosario |
| Antivirus | programas que permiten contar con medidas de protección efectivas cuando el equipo se encuentre expuesto a software malicioso o cualquier otro tipo de malware; Estos programas ofrecen la oportunidad de eliminarlo por completo o poner en estado de cuarentena. |
| Ciberseguridad | consiste en la protección y confidencialidad de sistemas e información. |
| Escáner de vulnerabilidades | software que detecta puntos frágiles en los sistemas informáticos de las empresas, con el objetivo de analizarlos y gestionarlos, dando respuesta oportuna a cualquier evento desafortunado. |
| Evento | cambio que no genera resultados negativos, un evento no trae implicaciones negativas, de este modo, puede ser usado como una expresión neutral. |
| *Firewall* | sistema cuya función es prevenir y proteger la red privada de ataques de otras redes. Su funcionamiento es sencillo: escanea los paquetes de red, permitiéndoles o bloqueándolos según las reglas definidas por un administrador. |
| *Hardware* | componentes físicos del computador, es decir, todo lo que se puede ver y tocar. |
| Incidente | representa resultados negativos. Pueden verse como las interrupciones o desmejoramiento en la calidad de los servicios prestados a los usuarios. Los incidentes deben atenderse mediante la estructura de gestión de incidencias. |
| Proxy | programa o dispositivo físico, que actúa de intermediario entre conexiones del navegador e internet, filtrando todos los paquetes entre ambos. Así mismo, establece un sistema de autentificación, que limita el acceso a la red externa, por lo cual, se puede generar los registros sobre sitios, visitas, y demás datos de navegación. |
| Riesgo | probabilidad que un evento desafortunado ocurra y genere consecuencias a una persona, entidad o cosa. |
| Seguridad de la Información | se encarga de proteger los datos contra robo de información, acceso no autorizado, obstaculización al sistema informático, manipulación y/o eliminación de datos. |
| Software | todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos. (Sistemas operativos, aplicaciones, etc.) |

**REFERENTES BIBLIOGRÁFICOS**

|  |  |
| --- | --- |
| **Tipo de recurso** | Bibliografía |
| Constitución Política de Colombia. Artículo 15 del 13 de junio de 1991 (Colombia). <https://dapre.presidencia.gov.co/normativa/normativa/Constitucion-Politica-Colombia-1991.pdf> | |
| Bsi group. (2022). Gestión de Seguridad de la Información ISO/IEC 27001. <https://www.bsigroup.com/es-CO/seguridad-de-la-informacion-isoiec-27001-/> | |
| Política nacional de explotación de datos (*Big Data*). CONPES 3920 del 2018 (Colombia). <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf> | |
| Política nacional de confianza y seguridad digital. CONPES 3995 del 2022. (Colombia).  <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf> | |
| Consulting Informático. (2016). Seguridad de la Información y Ciberseguridad ¿es lo mismo? <https://www.cic.es/seguridad-de-la-informacion-y-ciberseguridad-es-lo-mismo/> | |
| Reglamentó aspectos relacionados con la titularidad del uso de la información para el tratamiento de sus datos personales. Decreto 1377 del 26 de junio de 2012. (Colombia).  <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=48018#:~:text=El%20presente%20decreto%20tiene%20por,2002%2C%20adicionado%20por%20el%20art%C3%ADculo> | |
| DNP. (2020). *Guía normativa aplicable a la explotación de datos del 2020.* <https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/Documentos/Modelo%20Explotacion%20de%20datos/2.3%20Gu%C3%ADa%20normativa%20explotaci%C3%B3n%20de%20datos_VF.pdf> | |
| Gobierno de España. (2021). Las herramientas de análisis de datos más populares. <https://datos.gob.es/es/blog/las-herramientas-de-analisis-de-datos-mas-populares> | |
| Guía de Gestión de riesgos de seguridad de la información. (2021). El SGSI y la gestión del riesgo-Guía Icontec internacional de educación. Recuperado de <https://www.icontec.org> | |
| Hopkin, P. (2010). Fundamentals of risk management: understanding, evaluating, and implementing effective risk management. Londres, Reino Unido: Kogan Page Limited. | |
| Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2014). Tecnología De La Información: Técnicas De Seguridad. Gestión De Incidentes De Seguridad De La Información. Bogotá: ICONTEC. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/q6j6k0/sena_aleph000075887> | |
| Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2016). Gestión Del Riesgo: Orientación Para La Implementación De La NTC-ISO 31000 = Risk Management: Guidance for the Implementation of ISO 31000. Bogotá: Icontec.  <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000012244> | |
| Ley 1266. (2008). Por medio de la cual se dictan las disposiciones generales de habeas data (31 de diciembre de 2008). <http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html> | |
| Ley 1273. (2009). Modifica el código penal y crea como bien jurídico tutelado la protección de la información y de los datos (5 de enero de 2009). <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> | |
| Reglamentó aspectos relacionados con la titularidad del uso de la información para el tratamiento de sus datos personales. (2012). Decreto 1377. | |
| Ley 1581 de 2012. Principios y disposiciones que definen los derechos sobre los datos personales y denuncia de las violaciones de seguridad del 17 de octubre del 2012. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981> | |
| Razak,. M. F. Nor Badrul Anuar, R. S. and Ahmad, F. (2016). "The Rise of “malware”: Bibliometric Analysis of Malware Study." Journal of Network and Computer Applications 75 (2016): 58-76. Web. | |
| Bogotá: ICONTEC. (2014). Tecnología De La Información: Técnicas De Seguridad. Gestión De Incidentes De Seguridad De La Información. Print | |
| Toro, R. (2019). Estructura de la Norma ISO 27001:2013. [online] PMG SSI - ISO 27001. <https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura> | |
| Xataka Basics. (2017). Qué es un proxy y cómo puedes utilizarlo para navegar de forma más anónima. <https://www.xataka.com/basics/que-es-un-proxy-y-como-puedes-utilizarlo-para-navegar-de-forma-mas-anonima> | |

# **CONTROL DEL DOCUMENTO**

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

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

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