Guion para desarrollo de contenidos

**Datos de identificación del programa de formación**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Control de la seguridad digital |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica. | RESULTADOS DE APRENDIZAJE | Interpretar la política de seguridad y privacidad de la información según el modelo de negocio. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 2 |
| NOMBRE DEL COMPONENTE FORMATIVO | Fundamentos y normativa para la ciberseguridad. |
| BREVE DESCRIPCIÓN | Este componente formativo aborda conceptos y aspectos de la normativa y procedimientos básicos de la ciberseguridad en entornos corporativos, necesarios para garantizar el funcionamiento seguro de los procesos de la compañía, previniendo ataques cibernéticos a la información y/o datos vulnerables. Todos ellos, elementos que se realizan mediante buenas prácticas y procedimientos adecuados a las normas. |
| PALABRAS CLAVE | Ciberataque, ciberseguridad, seguridad, vulnerabilidad. |

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

# TABLA DE CONTENIDOS

Introducción

**1. Activos de información**

**2.** **Fundamentos de ciberseguridad**

2.1. Definición de conceptos esenciales

2.2. Contextualización y estado del arte

2.3. Objetivos de la ciberseguridad

2.4. Ciberseguridad: metodología, estrategias y técnicas de diagnóstico

**3. Normativa: ISO 27001**

3.1. Conceptos generales, principios y políticas

3.2. Técnicas y procedimientos de la norma

3.3. Gestión de riesgos y evaluación

**4.** **Manual de ciberseguridad corporativa**

**Introducción**

|  |
| --- |
| Cuadro de texto |
| Apreciado aprendiz, bienvenido a este componente formativo, donde se define la ciberseguridad, se reconocen los aspectos de importancia y aplicación real en la industria, los procedimientos y políticas que las empresas deben manejar, soportados en las normas internacionales sobre la gestión de la seguridad digital y, por último, un primer acercamiento a la identificación de amenazas, vulnerabilidades, acciones preventivas y correctivas en los sistemas de la compañía.  En el entorno empresarial los volúmenes de información que entran, salen y circulan son grandes e importantes; en ellos está presente gran parte de la información sensible y decisiva para garantizar el correcto funcionamiento y el cumplimiento de los objetivos organizacionales. Los datos están potencialmente expuestos a las amenazas existentes en las redes y sistemas digitales, solo el personal calificado y la correcta aplicación de los protocolos y normas pueden salvarlos y, por ende, a las empresas.  A través de vídeos, gráficos, imágenes y el contenido dispuesto en este recurso educativo, aprópiese de los conceptos necesarios para iniciarse en el mundo de la ciberseguridad.  En el siguiente video conocerá, de forma general, la temática que se estudiará a lo largo del componente formativo. |

**Guion de video introductorio**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tipo de recurso | Video animación 2D | | | |
| NOTA | La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente. | | | |
| **Título** | **Introducción a la Ciberseguridad, sus fundamentos y normativa.** | | | |
| Escena | Imagen | Sonido | Narración | Texto |
| 1 | En todas las escenas: ilustrar un personaje tipo expositor/profesor que narra, mientras en carrusel se muestran las imágenes de fondo, puede simular una empresa o ambiente de aprendizaje.  diseño del sitio web. desarrollo de tecnologías de programación y codificación. - personas enseñando seguridad digital fotografías e imágenes de stock | Se recomienda música instrumental de fondo. | Los ataques o delitos cibernéticos cada día son más frecuentes, y a diario se escuchan casos de víctimas que, por diferentes medios tecnológicos, han visto su información en peligro y con pérdidas económicas graves.  La seguridad en relación al uso de dispositivos y servicios digitales no puede ser un asunto de poca importancia, es alarmante la cantidad de peligros a los que la información está expuesta mientras se desarrollan actividades cotidianas como trabajar, estudiar y comunicarse. En la mayoría de los casos no se tiene la magnitud del alcance y consecuencias para una organización, incluyendo clientes internos y externos, lo cual es un tema de sumo cuidado, considerando que las empresas suelen contar con amplias bases de datos e información susceptible. | Ataques.  Delitos.  En la internet y la red.  Peligros a los que la información está expuesta |
| **2** | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ilustración conceptual de vector plano isométrico 3d de estafas de phishing de internet. - ataques ciberneticos |  | Mientras exista una conexión permanente al mundo digital, las empresas, organizaciones y personas se encuentran expuestas a la amenaza de hackers, virus informáticos, suplantación de identidad, robo y pérdida de información, entre otros riesgos.  Estos generan afectaciones con consecuencias económicas, retrasos en proyectos, obras y en general en la seguridad de los datos. | Amenazas:  Hackers, virus informáticos, suplantación de identidad, robo y pérdida de información. |
| 3 | el empresario dibuja el gráfico de crecimiento y el progreso de los negocios y analiza los datos financieros y de inversión, la planificación de negocios y la estrategia sobre un fondo azul. - aumento competitivo fotografías e imágenes de stock  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de diagrama de ventas - incremento de ventas  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de imán tirando gente para generación entrantes para símbolo de marketing digital - nuevos clientes |  | A pesar de estos riesgos potenciales, las empresas y personas necesitan de las redes de datos para ser competitivos y mantenerse vigentes en el mercado.  Ante esta situación, la mejor opción consiste en comprender el funcionamiento de los sistemas, identificar cuáles son los riesgos a los que están expuestos, conocer qué acciones ayudan a evitar los ataques cibernéticos y de ser atacados, saber cómo actuar. | Las redes de datos son útiles en las empresas para:   * Aumentar la competitividad. * Mantenerse vigente. * Realizar transacciones. * Comercializar. * Llegar a clientes de forma masiva.   Es necesario conocer los riesgos.  Diseñar estrategias de protección contra ataques cibernéticos. |
| 4 | iso 27001. estándar internacional de seguridad de la información. concepto de garantía de control de calidad de las normas iso - iso 27001 fotografías e imágenes de stock |  | A nivel mundial, organizaciones, empresas y gobiernos han dispuesto protocolos, estándares y normas entre estas se encuentra la norma internacional de Sistemas de gestión de seguridad de la información ISO27001, siendo el principal referente para la seguridad de la información, garantizando la calidad y veracidad de los procesos asociados a este.  Es necesario contar con tecnología de alto nivel, tanto en software como en hardware, que permitan reducir al mínimo los riesgos en los procesos que se llevan a cabo digitalmente. | Protocolos, estándares y normas.  Sistemas de gestión de seguridad de la información ISO27001. |
| 5 | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de gráfico iso 27001 con iconos y palabras clave - iso 27001 |  | Para adquirir el título de técnico del área de la seguridad digital, se debe de interpretar correctamente las políticas de seguridad adoptadas por la empresa, actuando conforme a estas normas y procedimientos.  Es necesaria la apropiación del concepto de ciberseguridad y su aplicabilidad en el contexto corporativo, comprender la importancia de las políticas de seguridad digital, interpretar y ejecutar los manuales de procedimientos existentes, proponer acciones motivadas a la actualización y mejoramiento de los mismos; todos estos necesarios para desarrollar una función efectiva y eficaz. | Interpretar políticas de seguridad.  Ejecutar los manuales de procedimientos.  Acciones de actualización y mejoramiento. |
|  | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de vector de actividad hacker - ataques ciberneticos |  | Aprender a interactuar con el grupo de trabajo en la misión de diseñar, ejecutar, evaluar el sistema y los procedimientos de seguridad digital de la compañía, es fundamental para prevenir y minimizar riesgos o solucionar incidentes de forma efectiva y colaborativa.  Se invita a estudiar el siguiente contenido, realizar las actividades, reflexionar sobre la importancia de la seguridad digital para empresas o personas, y los procedimientos en los ambientes donde deba realizar futuras labores. | Para proteger la organización de ataques cibernéticos debe:  Diseñar, ejecutar, evaluar el sistema y los procedimientos de seguridad digital. |
| Nombre del archivo | 233103\_CF02\_v1.mp3 | | | |

**Desarrollo de contenido**

1. **Activos de información**

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| Para iniciar con el contenido, es necesario conocer algunas definiciones oficiales básicas y, así, comprender más y mejor la temática que se abordará. La guía “**Metodología para la Identificación, Clasificación y Valoración de Activos de Información**”de la Súper Intendencia de Comercio, define un activo como “cualquier cosa que tiene valor para una organización”. El activo de información es definido como el “elemento de información que se recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre en forma impresa, escrita, en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes”. SIC(2018).  En relación con la seguridad de la información, la explica como cualquier información o elemento relacionado con el tratamiento de ésta que, tenga valor para la entidad, por ejemplo: archivos, bases de datos, expedientes, entre otros. | |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| Analice en detalle la definición que se propone en el siguiente esquema: | |

**Figura 1**

*Concepto de activos de conocimiento*

Activo de información

Se generan a partir de:

Todas las labores corporativas, sujetos y elementos que se involucren, produzcan o modifiquen información

Se incluyen como activos:

Información:

Escrita

Impresa

Almacenada digitalmente

Recursos

Software  
Hardware  
Bases de datos

Archivos

Personas

Equipos

Nota: resumen de conceptos activo de información. Producción del experto curricular (2022)

Para diseño del gráfico, a continuación el texto:

**Activo de información**

Se generan a partir de: Todas las labores corporativas, sujetos y elementos que se involucren, produzcan o modifiquen información

Se incluyen como activos:

Información: Escrita, impresa, almacenada digitalmente

Recursos: Software, hardware, bases de datos, archivos, personas y equipos

**Cod.Imagen:** 233103\_CF2\_i009

* 1. **Conceptualización de activos tecnológicos**

|  |
| --- |
| Cuadro de texto |
| Existen otros conceptos que se asocian a los **activos tecnológicos y de la información**, los cuales hay que conocer para comprender cómo se puede hacer una gestión eficiente de estos. |

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | Slider Presentación | |
| Introducción | Algunas definiciones de términos claves, referentes a los activos de la información con base en la guía “Metodología para la Identificación, Clasificación y Valoración de Activos de Información”, son: | |
| Archivo: es el conjunto de elementos, normas y procedimientos usados para conservar, proteger y clasificar la información generada en los procesos de la compañía. En informática también se conoce como archivo a cada uno de los documentos digitales con nombre y ubicación específica en la computadora o elemento de almacenamiento. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de trabajadores de office organizando el almacenamiento de datos y el archivado de archivos en el servidor o el equipo. usuarios de pc que buscan documentos en la base de datos. - archivo |
| Conocimiento corporativo: es aquel conocimiento que se le puede atribuir a una organización, el que posee esa organización. Este suele estar representado materialmente en algún tipo de documento. Las bases de datos adquiridas por una organización o la propiedad intelectual y las patentes que ésta desarrolla, son dos claros ejemplos de este tipo de conocimiento. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de mapa mental - conocimiento corporativo |
| Custodio: persona o parte que, dentro de sus funciones en la compañía, tiene la responsabilidad de administrar el uso y acceso a un determinado conjunto de información y garantizar su integridad. | | concepto de protección de la interfaz de firewall de seguridad cibernética. empresaria protegiéndose de los ataques cibernéticos. seguridad de datos personales y banca. - ciberseguridad fotografías e imágenes de stock |
| Integridad: cualidad, de la información, de estar completa y ser exacta. | | sistema de gestión documental (dms). software que automatiza el archivado y la gestión de archivos de datos. concepto de tecnología de internet. - información fotografías e imágenes de stock |
| Disponibilidad: característica, de la información, de estar accesible y utilizable según sea requerida. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de d2c direct to consumer, estrategia de ecommerce dirigida directamente al consumidor, tecnología de pantalla virtual - disponibilidad |
| Proceso organizacional**:** hace referencia a una dependencia o a un grupo, dentro de la organización, con funciones, actividades específicas y uno o más objetivos marcados. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ilustración conceptual de teambuilding. - proceso organizacional |
| Tecnología: agrupa el conocimiento, instrumentos o herramientas y técnicas para realizar una labor. | | primer plano del joven asiático comprando en la floristería. está pagando con su teléfono inteligente, escanear y pagar una factura en una máquina de tarjetas haciendo un pago rápido y fácil sin contacto. tecnología nfc, toque y vaya concepto - tecnología fotografías e imágenes de stock |
| Propietario del activo de información: es la persona, grupo de personas, dependencia u organización a quien se reconoce como autor y/o responsable de la seguridad y cuidado de una información en específico. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de archivo organizado. búsqueda de archivos en la base de datos. gestión de registros, registros y gestión de la información, documentos. - archivos |
| Recurso humano: recurso comprendido por el capital humano, sus conocimientos y habilidades para desarrollar una labor. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de fuente, tecnología de la información, documentos en concepto de base de datos. el trabajo en equipo del personal crea archivos de archivo y almacenamiento de datos en el servidor de la computadora - archivos |

* 1. **Caracterización y clasificación de activos tecnológicos**

|  |
| --- |
| Cuadro de texto |
| En relación con la **caracterización y clasificación de los activos tecnológicos**, destacan aquellos que hacen parte directa del proceso. Para lo cual, clasificarlos e identificarlos es una acción clave. |

|  |  |  |
| --- | --- | --- |
| Tipo  de recurso | Pestañas o tabs horizontales | |
| Introducción | A continuación, se describe cómo se clasifican: | |
| Información | * Bases de datos: conglomerados de información de los diferentes procesos de la organización. * *Backups*: copias de seguridad y respaldo de información valiosa que, por motivos de la organización, debe ser preservada y estar disponible para ser recuperada en caso de pérdida o daño. * Credenciales de acceso: contraseñas, información biométrica, *tokens* y llaves digitales para acceder a instancias especiales del sistema de información. * Aplicaciones y *Software* de uso corporativo**:** programas necesarios para ejecutar los procesos de la empresa. * Documentos almacenados en archivo físico. * Conocimiento de la operación**:** conocimiento de los procesos generado por los trabajadores. | mano de hombre de negocios con ordenador portátil moderno concepto cloud backup - backups fotografías e imágenes de stock |
| Activos físicos | * Equipos electrónicos:son computadoras y otros equipos terminales como *tablets*, teléfonos, entre otros. * Infraestructura de red: equipos como *routers*, *firewalls*, cableado, canalización, puntos de acceso, servidores y *racks*. * Equipos de almacenamiento digital:discos duros y memorias. * Recurso humano**:** personal, directivo, operativo, técnico, administrativo, que usa, guarda y genera conocimiento en la organización. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de conjunto de dispositivos isométricos vectoriales - equipos electronicos  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ilustración plana equipo de negocios investigación personas perfil para la contratación de empleo y entrevista en línea con concepto de reunión de videoconferencia - recurso humano |

* 1. **Gestión de activos tecnológicos: manejo, preservación y evaluación**

|  |
| --- |
| Cuadro de texto |
| Para realizar una gestión correcta de los activos tecnológicos se debe tener claridad sobre las características de cada uno de los elementos que integran el proceso de gestión. |

|  |  |
| --- | --- |
| Tipo de recurso | Acordeón tipo 2 |
| Introducción | Son tres los aspectos importantes relacionados con la gestión de los activos tecnológicos. |
| 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 - ciberseguridad | |
| * Manejo:es necesario que dentro de la organización exista una o más dependencias propietarias y custodios encargados del control y cuidado de los activos para llevar un registro de su uso, permisos de acceso, inventario, control de mantenimientos, copias de seguridad, rotulación, entre otras actividades relacionadas con el uso de los activos dentro de los diferentes procesos y actividades de la empresa. | |
| * Preservación: la organización deberá proveer los recursos y medios para salvaguardar la información, las políticas o normas relativas a esta actividad. En el caso de equipos electrónicos e infraestructura debe proporcionar la atención y mantenimientos preventivos, predictivos o correctivos que sean necesarios; deberá establecer los mecanismos e invertir en la tecnología y herramientas necesarias para asegurar la propiedad intelectual del conocimiento y el almacenamiento de la información producida por sus colaboradores, los instrumentos y procedimientos para almacenar datos tanto a nivel digital como físico, según sea el caso. | |
| * Evaluación:la compañía deberá establecer procedimientos para evaluar el estado de los activos tecnológicos, en aspectos como pertinencia, eficiencia, disponibilidad, tiempos, costos y funcionamiento en general. | |

1. **Fundamentos de ciberseguridad**

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| Para avanzar con el desarrollo del tema, es necesario tener claro el concepto de **ciberseguridad**. En este punto, haga una primera aproximación, prestando atención a los siguientes aspectos: | |

* 1. **Definición de conceptos esenciales**

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | Slider Citas | |
| Introducción | Diversos autores definen la ciberseguridad de la siguiente forma: | |
| Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020) definen la ciberseguridad así:  “conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información, vinculada a los usuarios de las cibertecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o recurso de valor para una persona, empresa u organización.  También, asocian los tres elementos que se observan en el gráfico: | | Ciberseguridad  Seguridad  Usabilidad  Privacidad  **Cod.Imagen:** 233103\_CF2\_i023 |
| Giant, N. (2016), indica que:  La ciberseguridad se refiere al uso seguro y responsable de los productos de la tecnología de la información y la comunicación (TIC), incluyendo Internet, los dispositivos móviles y de comunicación y los instrumentos tecnológicos diseñados para guardar, compartir o recibir información, por ejemplo, los teléfonos móviles, las cámaras digitales, etc.  Esta definición puede ampliar el concepto de ciberseguridad más allá de los antivirus y los equipos de seguridad de la red; hace énfasis en el usuario, la manera en que actúa y se responsabiliza sobre su propia seguridad y la de su empresa. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de hombre tratando de iniciar sesión en sus dispositivos, el usuario olvidó la contraseña, la seguridad web y cibernética con información de identificación incorrecta - ciberseguridad |
| La ciberseguridad agrupa recursos de *hardware* y *software* junto con políticas, normas y comportamientos seguros, los cuales tienen aplicabilidad para el uso personal, corporativo e industrial; siempre y cuando el personal cuente con formación sobre los cuidados que debe tener para proteger la información. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de el concepto de diseño planos de seguridad - ciberseguridad |

* 1. **Contextualización y estado del arte**

|  |  |
| --- | --- |
| Tipo de recurso | Tarjetas Conectadas |
| Introducción | Para continuar, es importante conocer el estado actual de la ciberseguridad en las empresas, el país y el mundo. |
| ciberseguridad y protección de la red con expertos en ciberseguridad que trabajan en internet de acceso seguro para proteger el servidor contra la ciberdelincuencia. persona escribiendo en el teclado de la computadora tarde en la noche - ciberseguridad fotografías e imágenes de stock | |
| ilustraciones, imágenes clip art, dibujos animados e iconos de stock de cyber de seguridad - crecimiento delitos ciberneticos | Crecimiento exponencial:citando nuevamente aArroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020), “en España, por ejemplo, en solo un año, entre 2018 y 2019, los ciberdelitos denunciados representaron un 10% del total de denuncias por algún tipo de delito, y en este mismo periodo se tuvo un aumento del 35% de los casos reportados”. |
| bandera de colombia en la computadora - delitos en colombia fotografías e imágenes de stock | En Colombia:según cifras del Centro Cibernético Policial MinTIC (2021), durante el año 2021 los delitos cibernéticos ascendieron a 33.465, lo que significa un aumento de 17% en comparación con 2020, cuando fueron 28.524 casos. Además, se recibieron 1.558 denuncias y se efectuaron 49 capturas. |
| concepto de los costes de las infraestructuras de la información - ciberseguridad precio iconos fotografías e imágenes de stock | El precio de los fallos en ciberseguridad**:** la revista portafolio (2022), indica que, en el mundo, durante el último año, los ciberdelitos crecieron en un 150% y, aproximadamente, el 32% de las empresas fueron atacadas. Estas se vieron en la obligación de pagar rescates a piratas informáticos para recuperar su información. Entre esas empresas se encuentran corporaciones, bancos e, inclusive, gobiernos, por lo cual tales pagos representan cantidades de dinero considerables. |
| ley de normas de cumplimiento e interfaz gráfica de regulación para la política de calidad empresarial - politica norma fotografías e imágenes de stock | Políticas públicas: según MinTIC (2021), el propósito de la política de seguridad digital es que las personas y las empresas conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan cómo protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.  Esta labor a nivel institucional requiere un arduo trabajo e inversión conjuntas entre el estado y la empresa privada, labor que tiene un alto componente educativo que exige adoptar una cultura de seguridad digital en el país. |

* 1. **Objetivos de la ciberseguridad**

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | Infografía interactiva Punto caliente | |
| Texto introductorio | A pesar de los riesgos y las cifras alarmantes, la ciberseguridad ha sido considerada como prioridad para las organizaciones, los gobiernos y las personas, estableciendo propósitos u objetivos de las políticas de esta:  **Figura 2**  *Objetivos de la ciberseguridad* | |
| . | | |
| Código de la imagen | Cod.Imagen: 233103\_CF2\_i031 | |
| Punto caliente 1 | La cultura digital de las personas tiene alto impacto en el desempeño de un sistema de seguridad digital, por eso es fundamental que la ciberseguridad se enseñe desde temprana edad en los colegios y sea tema de constante capacitación para profesionales y empresas. | Al lado o ligado a la palabra: sensibilización y educación. |
| Punto caliente 2 | La ciberseguridad es un área del conocimiento que actualmente tiene una demanda alta de profesionales y provee mejores salarios, con respecto a otros cargos del entorno de las TIC. | Al lado o ligado a la palabra: empleo. |
| Punto caliente 3 | La ciberseguridad requiere que se invierta en investigación y desarrollo de tecnologías capaces de actuar y proteger de las amenazas modernas, que evolucionan también a un ritmo acelerado. | Al lado o ligado a la palabra:desarrollo tecnológico. |
| Punto caliente 4 | La protección es el objetivo más evidente de las políticas de seguridad digital. Los más protegidos son los activos de información de las empresas, ya que ellos son la fuente principal del movimiento operativo y económico de las organizaciones. | Al lado o ligado a la palabra: protección. |
| Punto caliente 5 | En la medida en que el sistema de la organización esté blindado de ataques, podrá garantizar una mayor seguridad a los usuarios, asegurando menos riesgos y reprocesos, lo que se verá reflejado en mayor eficiencia y menor probabilidad de tener que pagar rescates a delincuentes informáticos. | Al lado o ligado a la palabra: economía. |

* 1. **Ciberseguridad: metodología, estrategias y técnicas de diagnóstico**

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| En la ciberseguridad es necesario plantear estrategias que se desarrollen a través de métodos y metodologías que marquen la ruta por seguir, cómo garantía de seguridad digital de la información en la organización. En el siguiente vídeo se detallan las metodologías y estrategias. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tipo de recurso | Video animación 2D | | | |
| NOTA | La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente | | | |
| Título | Metodología y estrategias de la ciberseguridad | | | |
| Escena | Imagen | Sonido | Narración | Texto |
| 1 | Al ser un vídeo donde se presenta una lista de estrategias, se propone un personaje disfrazado de héroe “Ciberseguridad”.  Se debe narrar y complementar con las imágenes de cada escena.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de software antivirus metáfora ilustración vectorial de estilo de diseño plano - ciberseguridad heroe  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de carpeta de espías - archivos sospechosos | Sonidos de fondo que representen alertas de acuerdo a cada escena. | En este vídeo se exponen algunas estrategias básicas de ciberseguridad, para garantizar la seguridad digital es necesario implementarlas. El Ministerio de las TIC -MinTIC presenta algunas recomendaciones:   1. No descargar archivos sospechosos: evite descargar archivos como ejecutables, cracks, programas de los que no tiene referencia o su autor no es reconocido, descargue solo a través de páginas de confianza o directamente de los fabricantes y proveedores autorizados. | No descargar archivos sospechosos. |
| 2 | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de software de actualización del sistema cambio de nueva versión. instalación de proceso de actualización, programa de actualización, instalación de red de datos, icono plano, adecuado para página de destino web, banner, plantilla vectorial - actualizar software  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de mantenimiento informático - antivirus |  | 1. Actualizar el software del sistema periódicamente: es necesario para corregir fallos, vulnerabilidades y mejorar la seguridad del equipo. 2. Usar antivirus y aplicaciones anti-malware: sean pagos o gratuitos se debe buscar una buena opción para el equipo, mantener actualizado el antivirus y evitar instalarlos en versiones antiguas o que sean activados de manera fraudulenta; actualmente la mayoría de los antivirus son ofrecidos en sus versiones pagas. | Actualizar el software del sistema periódicamente.  Usar antivirus y aplicaciones anti-malware. |
| 3 | concepto de seguridad en internet, acceso de usuario, inicio de sesión y contraseña en la computadora - contraseñas fotografías e imágenes de stock  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de sesión equipo multitarea - cerrar la sesión |  | 1. Crear mejores contraseñas y cambiarlas cada seis meses: realizar una gestión en las contraseñas, aunque sean difíciles de recordar es clave, en estas se recomienda incluir códigos de acceso con alto nivel de complejidad para ser indescifrables por terceros. 2. Acostumbrar a cerrar las sesiones al terminar: se recomienda cerrar sesión si no se encuentra en el equipo personal, muchas plataformas muestran las sesiones que se encuentran abiertas y en que equipos. | Crear mejores contraseñas y cambiarlas cada seis meses.  Acostumbrar a cerrar las sesiones al terminar |
| 4 | concepto de conexión en línea compartir red social - redes publicas fotografías e imágenes de stock  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de personas desconectándose y haciendo una desintoxicación digital - desconectarse de internet |  | 1. Evitar operaciones privadas en redes abiertas y públicas: para realizar transacciones y actividades de carácter privado e importante, se debe hacer a través de conexión en redes de confianza o privadas (que usen contraseña). Se recomienda verificar en el apartado de redes las carpetas y archivos que se encuentran habilitados para compartir mediante red local. 2. Desconectarse de internet cuando no se necesite: si no es necesario, y esto es muy común en muchas empresas, se sugiere no usar internet a nivel corporativo, el uso de internet debe ser restringido o trabajar mediante intranets. | Evitar operaciones privadas en redes abiertas y públicas  Desconectarse de internet cuando no se necesite |
| 5 | concepto de tecnología de computación en la nube, mano utilizando portátil con datos de carga en el almacenamiento de internet. - copias de seguirdad fotografías e imágenes de stock  navegador web oscuro primer plano en la pantalla lcd con enfoque superficial en el candado https - paginas seguras fotografías e imágenes de stock |  | 1. Realizar copias de seguridad: se aconseja guardar copias de respaldo en los medios más convenientes o autorizados por la empresa, según la importancia de la información y las políticas de esta. 2. Navegar por páginas web seguras y de confianza: se sugiere hacer uso de páginas confiables y con certificado https, evitar páginas de reputación dudosa con ventanas emergentes y publicidad en exceso. | Realizar copias de seguridad  Navegar por páginas web seguras y de confianza |
| 6 | concepto de negocio de red. red de comunicación. - red wifi segura fotografías e imágenes de stock  puntos de dedo para botón derecho del ratón de ordenador de contacto aislado - clic en enlaces raros fotografías e imágenes de stock |  | 1. Comprobar la seguridad de la red WIFI: actualice con frecuencia las contraseñas de sus redes personales y aprenda a identificar qué otros equipos se conectan constantemente. 2. No hacer clic en enlaces extraños: evitar dar clic en promociones, ofertas o premios en los que nunca ha participado. | Comprobar la seguridad de la red WIFI  No hacer clic en enlaces extraños. |
| 7 | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de protección de datos personales - datos personales  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de firma digital, protección de datos, términos y condiciones establecidos. empresarios firmando contrato con firma electrónica. el especialista cibernético protege los archivos con una contraseña segura. el usuario acepta el acuerdo de política de priv - datos personales  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de seguridad y salud en el trabajo. un hombre con casco de construcción con un documento sobre fondo blanco. - politica de seguridad |  | 1. No brindar datos personales a desconocidos: no suministrar información personal en páginas o a personas ajenas. 2. Separar las actividades personales de las laborales: en sus cuentas de correo, redes sociales y en el uso de software, siempre que sea posible usar diferentes dispositivos. 3. En las empresas se debe hacer una política de seguridad corporativa: conocer y cumplir la política de seguridad digital de la empresa. | No dar datos personales a desconocidos  Separar las actividades personales de las laborales  Política de seguridad corporativa |
| Nombre del archivo | 233103\_CF02\_v2.mp3 | | | |

**Técnicas de diagnóstico**

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | | Pestañas o tabs Verticales |
| Introducción | | El proceso de ciberseguridad requiere la aplicación de acciones y procedimientos de identificación del estado del sistema de información digital y de los equipos.  La **vulnerabilidad** es un punto débil del sistema desde el cual un tercero o una persona malintencionada puede acceder a la información. Una manera útil de diagnosticar la seguridad de este, consiste en ubicarse en el lugar de quien quiere perjudicar el sistema e intentar acceder y afectar algún elemento.  Se sugiere considerar las siguientes preguntas y sugerencias, si en alguna la respuesta es positiva o existe una alternativa, se identifica una vulnerabilidad en el sistema. |
| equipo diverso de profesionales que se reúnen en la oficina por la noche: lluvia de ideas los programadores de ti usan la computadora juntos, hablan de estrategia, discuten la planificación. ingenieros de software desarrollan un programa de aplicaciones  - ciberseguridad fotografías e imágenes de stock  mujer uso de la aplicación bancaria en la factura de servicios públicos de pago de teléfonos inteligentes, concepto de banca por internet de tecnología financiera - ciberseguridad fotografías e imágenes de stock | | |
| A nivel físico | ¿Qué tan probable será que un tercero acceda físicamente a algún equipo o terminal, viole el acceso y pueda extraer, modificar o eliminar información importante?  Verifique los permisos de acceso a carpetas, archivos y cuentas de usuario, por ejemplo, ¿qué tan seguras son las contraseñas? | |
| A nivel de conectividad | ¿Qué probabilidad tiene y de qué forma podría un tercero acceder de manera inalámbrica o mediante cable a alguna de las redes o equipos de la compañía y, estando allí, qué información podría estar a su alcance?  Verifique la seguridad de las contraseñas y el listado de equipos conectados a los medios inalámbricos, identifique qué puertos podrían estar potencialmente disponibles para la conexión de un tercero en los equipos de red y el control de acceso al cuarto de telecomunicaciones. | |
| Software | ¿El *software* que tiene la compañía, cuenta con las licencias correspondientes o se usa de manera ‘pirata’? ¿los equipos de la empresa tienen instalados solo los programas permitidos y en sus versiones autorizadas? o ¿existe algún equipo con software de terceros instalado sin autorización?  Compruebe el listado de programas instalados y la lista de procesos en ejecución de cada equipo. | |
| Físico/locativo | Los activos ¿están expuestos a algún factor ambiental, físico o humano que pueda ocasionar daños o pérdidas en los equipos y la información?  Revise las instalaciones eléctricas, niveles de voltaje, protecciones, sistemas contra incendios, extintores, sustancias, equipos o procedimientos riesgosos cerca de estos. | |
| Factores humanos | ¿Cuánto conocen las personas que manejan información en la empresa? ¿Qué nivel de formación y cualificación tiene el personal para favorecer la seguridad de la información?  Evalúe el nivel de conocimiento y ejecución de la política de seguridad digital de la empresa, capacite a las personas en el correcto uso de los equipos y el manejo de la información. | |

1. **Normativa: ISO 27001**

|  |  |
| --- | --- |
| **Tipo de recurso** | **Slider Citas** |
| **Introducción** | Este apartado le mostrará detalles y aspectos clave sobre la reglamentación de la norma ISO 27001. |
| **¿Qué es la ISO 27001:2013?**  Es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como el cumplimiento legal. La certificación ISO 27001 es esencial para proteger los activos más importantes en la organización, la información de los clientes y empleados, la imagen corporativa y otra información privada. La norma ISO incluye un enfoque basado en procesos para lanzar, implantar, operar y mantener un SGSI. | **https://lh3.googleusercontent.com/baKexJKWxQXJn-7NByAAjFaxaYCZnWd7SsEohGS4Zs8p7V3vg9vyHe3T_3H1OYS6GkYH6jqclSeaJ70Y2JJPbPRZQWwn3kGeLfHyLfL7YECITcU5pjsyonXNL7ct8ilID9mErhVtyXJJNHTGA-q6LEa5kS8DEAX3clYLsz2c8yZ0Wi1qIpTbuZUoyLU3** |

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| **Guía de implantación nqa**  Para ampliar la información anterior sobre la implantación de la ISO 27001, ver el documento.  **Descargar**   Anexo 1: guia\_de\_implantación\_nqa | |

* 1. **Conceptos generales, principios y políticas**

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | Slider pasos | |
| Introducción | La norma ISO 27001 hace parte de la familia de normas ISO27000, conozcamos algunos aspectos importantes sobre ellas: | |
| Slide 1 | ISO 27000 Tecnologías de la información – Resumen y vocabulario | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de insignia certificada estándar de seguridad de la información iso 27000 - iso 27000 |
| Slide 2 | ISO 27001 es la norma destinada a la certificación de las empresas en gestión de seguridad de la información (SGSI). | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de iso 27001 banner vectorial verde certificado. etiqueta de certificación plana aislada sobre fondo blanco. concepto de seguridad alimentaria. ilustración vectorial. - iso 27001 |
| Slide 3 | ISO 27002 Tecnologías de la información– Técnicas de seguridad – Código para prácticas en materia de controles de seguridad de la información. Es la norma más referenciada y está ligada al diseño e implantación de los 114 controles especificados en el Anexo A de la ISO 27001. | concepto de iso. control de calidad. normas - iso 27001 fotografías e imágenes de stock |
| Slide 4 | ISO 27005 Tecnologías de la información– Técnicas de seguridad – Gestión de la seguridad de la información. | certificación iso estandarización concepto de control de calidad en pantalla. ilustración 3d - iso 27001 fotografías e imágenes de stock |
| Slide 5 | La norma es revisada cada 5 años, la norma referente para obtener la certificación internacional es la versión 2013. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de tres jóvenes personajes femeninos presentan el certificado iso 27001 con sello - iso 27001 |
| Slide 6 | La implementación de las políticas mencionadas en esta norma tendrá un impacto positivo en el sistema de información digital de la compañía, en la imagen y confianza que trasmitirá a los colaboradores internos y usuarios de la misma. | estudio del componente legal para el desarrollo de un negocio. - leyes fotografías e imágenes de stock |
| Slide 7 | Su aplicación servirá como ventaja competitiva, le permitirá a la empresa aplicar a ofertas y contratos con terceros, incluidas organizaciones del gobierno donde es requisito cumplir con esta certificación. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de estadísticas de ordenador - ciberseguridad competencia |

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | Carrusel de tarjetas | |
| Introducción | El desarrollo de la norma se basa en los siguientes principios esenciales, sobre los cuales se alcanza el objetivo de proteger los activos de la información: | |
| Imagen: r15\_i1.png | | |
| * Proteger los activos de la empresa, lo que incluye personas, información, capital y equipos. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de protección de ilustración vectorial degradado estilo colorido. - seguridad digital iconos |
| * Identificar y corregir las vulnerabilidades a la seguridad de los activos. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de icono de detección ocular o reconocimiento ocular - seguridad informatica iconos |
| * Diseñar e Implementar los manuales de procedimientos para la gestión de los activos de manera segura. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de línea blanca icono manual de usuario aislado con sombra larga. guía del usuario. signo de instrucción. lea antes de usar. botón de círculo rojo. ilustración vectorial - manuales iconos |
| * Establecer los procedimientos y el manejo de contingencias y emergencias asociadas a la seguridad digital. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de icono de manual de instrucciones. páginas de libro abierto con texto, imágenes y mano puntero cursor el símbolo. - procedimientos iconos |
| * Proteger la confidencialidad, integridad y disponibilidad de la información. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de autenticación y seguridad cibernética - confidencialidad de información iconos |

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | | Pestañas o tabs Verticales |
| Introducción | | La norma se ejecuta mediante 10 etapas o cláusulas, a continuación, se realiza una breve descripción de cada una: |
| ilustraciones, imágenes clip art, dibujos animados e iconos de stock de icono de firma de contrato o documento. documento, carpeta con sello y texto. condiciones del contrato, aprobación de la investigación - politicas iconos | | |
| Cláusula 1 - Alcance | La norma ha sido diseñada para ser aplicable en todas las empresas, independientemente del sector al que pertenezca y tamaño de la misma. | |
| Cláusula 2 - Base normativa | La certificación incluye la aplicación de los parámetros de la familia de normas ISO 27000. | |
| Cláusula 3 - Definición de conceptos clave | Se debe incluir la definición de palabras y elementos claves contenidos en la norma ISO 27000. | |
| Cláusula 4 - Contexto de la organización | Incluye el análisis del entorno organizacional, proceso y estudio de las vulnerabilidades, además de las necesidades de cada una. | |
| Cláusula 5 - Liderazgo y definición de roles | Se establece la distribución de responsabilidades respecto al sistema de seguridad digital de la organización. | |
| Cláusula 6 - Planificación e identificación de riesgos | Se plantea la proyección de riesgos. | |
| Cláusula 7 - Soporte | Se definen los recursos técnicos, humanos y económicos destinados a la implementación y ejecución del sistema de seguridad digital. | |
| Cláusula 8 - Operación | En esta fase se definen los parámetros y políticas para la ejecución del sistema de seguridad digital. | |
| Cláusula 9 - Evaluación | Se realiza la valoración de los resultados del sistema. | |
| Cláusula 10 - Mejora | Planteamiento de acciones correctivas y de mejoramiento basados en la evaluación de resultados de la ejecución del sistema de seguridad digital. | |

* 1. **Técnicas y procedimientos de la norma**

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | Infografía interactiva Punto caliente | |
| Texto introductorio | Para la implementación de la norma hay dos aspectos importantes a tratar: la metodología de planeación, ejecución y evaluación, además de las auditorías al sistema. En el siguiente gráfico se describe el método PHVA, una de las metodologías más usadas. | |
| Imagen  **Figura 3**  *Ciclo PHVA, Planear – Hacer – Verificar - Actuar* | | |
| Código de la imagen | Cod.Imagen**:** 233103\_CF2\_i062 | |
| Punto caliente 1 | Ciclo PHVA: se implementa a través del método PHVA, (planear, hacer, verificar, actuar), como está registrado en el orden lógico de las 10 cláusulas. | En cada uno de los nombres que están en la imagen. |
| Punto caliente 2 | Planear: analizar y establecer los objetivos, recursos y procedimientos para la implementación. |  |
| Punto caliente 3 | Hacer: ejecutar las acciones formuladas en la planeación. |  |
| Punto caliente 4 | Actuar: establecer acciones de mejora y actualización. |  |
| Punto caliente 5 | Verificar: evaluar los resultados y funcionamiento del sistema e identificar vulnerabilidades. |  |

**Auditorías**

|  |  |
| --- | --- |
| Tipo de recurso | Acordeón tipo 1 |
| Introducción | Es el método por el cual se verifica el correcto desarrollo de un proceso, se evalúa la adecuada ejecución de la metodología, instrumentos y políticas establecidas por la norma de referencia y se identifican las falencias o puntos por mejorar. |
| ilustraciones, imágenes clip art, dibujos animados e iconos de stock de contabilidad y contabilidad. personajes de contadores diminutos en enorme clip board llenando datos de contabilidad, gráficos y gráficos - auditoria | |
| Auditoría interna:  Es realizada por el personal interno de la empresa, su objetivo es identificar fallos en una primera instancia y preparar las auditorías externas para certificar la norma. | |
| Auditoría externa:  Se contrata o solicita la revisión de uno o varios auditores externos e independientes a la empresa, para dar su concepto técnico y hallar fallos. | |
| Auditoría de certificación:  La realiza un organismo acreditado para certificar la implementación de la norma donde se evaluará el cumplimiento de esta, en dicha auditoría todo debe estar funcionando según los parámetros, ya que no hay oportunidades de corrección. | |

* 1. **Gestión de riesgos y evaluación**

|  |  |
| --- | --- |
| **Tipo de recurso** | **Carrusel de tarjetas** |
| **Introducción** | A continuación, se amplía la explicación de la **planeación y evaluación de riesgos**: |
| **Imagen general que ilustre el tema (opcional)** | |
| Para el SGSI (Sistema de Gestión de Seguridad de la Información) es vital en su etapa de planeación identificar los riesgos. | **https://lh6.googleusercontent.com/DFtxm_P2zyr2lJcVOfyFsKTLIWBvf53n51ECxYjSd7Y8cgMIRRFQ1FDM5ooRAN9pqsSODQrxD3gn4AzHm9fdJAuAGHpIcHb0oP6YU7aPd4FpoCpaHkz0oPv31q7T84OElHbJAuWapSVIPx0dPkmskX4tQqDwaUsdp0x5hA-RxXeLpaGyn0gnMSQyNGCO** |
| Siempre existirán riesgos, lo que se puede controlar es la probabilidad de que ocurra un incidente. | **https://lh4.googleusercontent.com/XZPGsAQEporKPpOSRTPDfflWXdCYYTTCluLRxmZ4YQCjUyDshHof6uXH9Lv3_6tGE2P0eiSNOxfEgzvMqj1K4lNuffRWzYhcpGy0fkqKIZ4nZvxtXjxDSzCZURHEljkwU497AgcWBh5GAACtkeQYzI_WSo6xIzWS2U9Am9COamAIfwkL3gEQN8WM2HMt** |
| Es posible que existan riesgos que para el contexto y recursos de la organización no se puedan solucionar aún. | **https://lh3.googleusercontent.com/3Mgk361LYlSGTM7KyUCcuuHyeJAxbjf_z3J0yX-a--ZDUKLT1XlfGKqrn7bKF8965bNXIPivzfxGlw8mdeEv3YJl-197oJTcmAd-79DXIyBW5ZDDDdPs2QUTiU33U8hY5PckqhqQYraocc1x7ruhuzVlIWha9m1Q1HTmtFp2S8P0Qve9vCYuh-ltLfg-** |
| Se deben caracterizar o clasificar los riesgos según el tipo de activo que pueden afectar e identificar las posibles soluciones o métodos para reducir su probabilidad o impacto. | **https://lh4.googleusercontent.com/f8P7HCLOuW7vIv3ly8bx9Nt2CPuMObjj_ZRqBEpHyQXqdAWs_GM_VSjC8mYSTfyjMFJFCFJXMUBu9Dec21l5HfGleJUQSmyk_t7-f0AdivxmPbLB9xnikLlnaXp7bIsuVKPQEevaDg-7blP5I6Q2VOOhgHlRusbW4qHzfxpCXfW0x7uGsIhWlB4C3bau** |

* 1. **Evaluación y administración.**

|  |  |
| --- | --- |
| Tipo de recurso | Rutas / Pasos. Verticales 1 |
| Introducción | La evaluación y administración del sistema es el único método para validar que tan efectivo es. |
| ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de encuesta en línea. personajes masculinos y femeninos pequeños que llenan el formulario digital en la enorme aplicación de computadora portátil y smartphone - evaluación | |
| Botón 1 | Se evalúan los resultados obtenidos en material de seguridad, incidentes ocurridos e incidentes evitados. |
| Botón 2 | Se valora el impacto del sistema en cuestión de costos en recursos económicos, humanos, tiempo y procesos. |
| Botón 3 | Se establecen las metas, puntos a corregir o agregar al SGSI. |
| Botón 4 | El sistema se administra con base en el manual de procedimientos establecido por la empresa. |

1. **Manual de ciberseguridad corporativa**

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| Un manual de procedimientos es un documento escrito donde se reglamenta y se especifica la manera aprobada por la empresa para realizar determinada labor, cómo deben realizarse los procedimientos y la información de manera organizada y continua dentro de la empresa.  Todo empleado deberá aplicarlos en su labor diaria para evitar sanciones y evitar alterar la calidad, seguridad y funcionamiento del sistema completo de la compañía. | |

|  |
| --- |
| Cuadro de texto |
| **Manual de procedimientos departamento de sistemas dif estatal chihuahua**  Se recomienda revisar el Anexo 2 Manual de procedimientos departamento de sistemas dif estatal chihuahua, para reconocer el contenido y metodología de un manual de procedimientos.  Botón: **Descargar** |

* 1. **Objetivos y alcance**

|  |  |
| --- | --- |
| Tipo de recurso | Cajón de texto de color |
| Se deben plantear los objetivos específicos teniendo como referente el alcance del manual, este debe ser documentando de la siguiente forma:   * Alcance: todo cargo o actividad de la empresa debe tener establecidas unas responsabilidades y procedimientos estandarizados: desde los niveles más bajos con el personal auxiliar y operativo, pasando por el personal técnico, ingeniería, personal administrativo y llegando hasta los altos cargos directivos. Se debe tener un manual de procedimientos, algunos de carácter general, mientras otros son específicos para cada labor. * Objetivos   - Delimitar labores y referentes a un cargo específico.  - Imponer los pasos para realizar una actividad.  - Establecer con detalle las funciones, actividades y temas que pueden generar controversias o discusiones.  - Garantizar la seguridad, buenas prácticas y uso adecuado de los activos de la empresa.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de objetivo del negocio. planificación de tareas. objetivos de trabajo. gente diminuta con una enorme puntería redonda y una flecha de diana. infografía de progreso. logro de empresario. trabajo en equipo y gestión del trabajo. concepto vectorial - objetivos | |

* 1. **Estructura organizacional**

|  |  |
| --- | --- |
| Tipo de recurso | Acordeón tipo 2 |
| Introducción | La estructura organizacional, la cual también se contempla en el manual, tiene los siguientes elementos: |
| ilustraciones, imágenes clip art, dibujos animados e iconos de stock de información secreta 3d. los datos confidenciales se cierran con un candado. documento en papel, información prohibida. el concepto de autorización, entrada verificada, acceso, código seguro. resultados de la encuesta cerrada. vector - manual de ciberseguridad | |
| Organigrama de la empresa: toda empresa está compuesta por un grupo de colaboradores con un cargo y responsabilidades predefinidas, conocer cómo es la organización de esta, facilita la canalización de la información para que llegue a quienes son competentes en el tema y para evitar que se comparta o se generen confusiones, al llegar a quienes no les resulta relevante dicha información. | |
| Conducto regular y canales de comunicación: la empresa establece los canales para la comunicación formal y las líneas de supervisión o mando para transmitir la información. | |
| Roles y cadena de mando: cada empleado tendrá sus funciones y límites establecidos, además de un jefe inmediato para canalizar toda información o requerimiento. | |

* 1. **Lineamientos y políticas corporativas**

|  |  |  |
| --- | --- | --- |
| Tipo de recurso | Slider pasos | |
| Introducción | La empresa necesita definir los **lineamientos y políticas corporativas** sobre las cuales trabajará, en el campo de la seguridad digital. Algunas políticas establecidas son: | |
| Slide 1 | Entrada y salida de equipos informáticos y planta física perteneciente a la empresa. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de monitor con un tablero y un personaje masculino con un lápiz gigante. productividad personal, horario, informe de desempeño de los empleados. ilustración plana vectorial. - equipos informaticos |
| Slide 2 | Correo electrónico. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de suscríbete a la newsletter. ilustración vectorial para marketing online y negocios. sobre abierto con carta en el teléfono. regístrese en la lista de correo. ilustraciones vectoriales web en 3d. - correo electronico |
| Slide 3 | Criterios para la asignación de permisos de acceso a archivos y carpetas, creación y actualización de contraseñas. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de retrowave ui y elementos ux - correo electronico |
| Slide 4 | Sistema de gestión documental para el control del flujo de información. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de diagrama de flujo de la tecnología inalámbrica de red 5g. torre de comunicación, servidor, portátil, smartphone, ilustración isométrica vectorial - flujo de información |
| Slide 5 | Instrumentos y protocolos para actividades concretas como la comunicación, solicitud de suministros, elaboración y presentación de informes, entre otros. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de vector de estudiantes que aprenden en línea en casa mediante la capacitación en seminarios web - protocolos |
| Slide 6 | Uso de los activos. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ilustración vectorial del concepto de la industria 4.0. flat modern design for web page, banner, presentation, etc. - activos informaticos |
| Slide 7 | Manejo e instalación de *software*. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de soporte remoto en línea. acceso remoto y control de escritorio de computadoras o laptop a través de conexión a internet web. el administrador del sistema ayuda a los clientes, los empleados solucionan problemas, software de instalación y equipos. - manejo de instalación de software |
| Slide 8 | Periodicidad para la creación sobre copias de seguridad, actualización de inventarios y disposición final o eliminación en activos sacados de circulación. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de metáforas de concepto vectorial de plataforma de alojamiento web. - copias de seguridad |
| Slide 9 | Uso de dispositivos electrónicos dentro de las instalaciones de la compañía. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de alojamiento web isométrico 3d, concepto de servidor de red de base de datos. ilustración vectorial de ingenieros de servidores de tecnología de red en la nube. el mantenimiento del servicio de equipos de servidor - copias de seguridad |
| Slide 10 | Acceso y limitaciones al servicio de internet. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de personas diminutas con cuenta bajo bloqueo en la pantalla de la computadora portátil - ciberseguridad |

|  |
| --- |
| 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**

|  |  |
| --- | --- |
| Tipo de recurso | Síntesis |
| Técnico en control de la seguridad digital.  Síntesis: CF2-Fundamentos y normativa para la ciberseguridad. | |
| Introducción | El siguiente mapa integra los criterios y especificidades de los conocimientos expuestos en el presente componente formativo. |
| **Texto para el diseñador web**  Ciberseguridad  Concepto  Conjunto de políticas para proteger los activos de información  Activo de información  Información en medio digital y físico  Conocimiento del personal – colaboradores  Herramientas tecnológicas  Infraestructura  Normativa  Políticas de la empresa  Manual de procedimientos y políticas de seguridad digital  ISO 27000  Conjunto de normas internacionales para la certificación y gestión en seguridad de la información (SGCI)    Buenas prácticas  Administración de permisos, accesos y contraseñas  Implementación de procesos y tecnologías  Uso de software autorizado y legal  Uso responsable y seguro de internet  Copias de seguridad, periódicas y frecuentes  Conocimiento y aplicación de las políticas internas  Imagen:233103 CF2\_\_i077 | |

Actividad didáctica

|  |  |
| --- | --- |
| **Tipo de recurso** | Actividad didáctica. Verdadero y falso |
| Apreciado aprendiz, a continuación encontrará una serie de preguntas que deberá resolver, con el objetivo de evaluar la aprehensión de los conocimientos expuestos en este componente formativo. | Free illustrations of Check mark |
| **El Recurso humano está incluido dentro de los activos de la empresa** | Negociación salarial, discusión sobre aumento salarial o acuerdo de salarios y beneficios, acuerdo comercial o concepto de fusión y adquisición - arte vectorial de Salarios libre de derechos |
| Verdadero (correcto),  Retroalimentación += ¡Muy bien!, las personas y sus conocimientos sobre las actividades son un recurso muy valioso para la empresa. | Falso (incorrecto)  Retroalimentación -= Se debe considerar a las personas, su conocimiento, dominio de las técnicas y procesos como un activo útil y valioso de la empresa. |
| **El propósito de realizar copias de seguridad, es garantizar una copia reciente de la información en caso de que la original se pierda o se dañe.** | el disco duro se está quemando - burn disc fotografías e imágenes de stock |
| **Verdadero (correcto)**  Retroalimentación +=Muy bien, se deben realizar copias de seguridad con frecuencia para disminuir el impacto que puede ocasionar la pérdida de información. | Falso (incorrecto)  Retroalimentación -= Es necesario que se realicen con frecuencia copias de seguridad para evitar pérdida de grandes volúmenes de información en caso de daño de la versión original. |
| **Las contraseñas corporativas deben ser compartidas al jefe inmediato** | Formulario en línea de contraseña. Imagen conceptual de ciberseguridad. - Foto de stock de Contraseña libre de derechos |
| Verdadero(incorrecto)  Retroalimentación -=Las contraseñas son de carácter personal, ni aun con el jefe inmediato deben ser compartidas; hacerlo, puede desencadenar problemas e irregularidades en los procesos. | **Falso (correcto)**  Retroalimentación += Muy bien, la contraseña es de carácter personal y para evitar todo tipo de problemas no debe ser compartida con ningún otro miembro de la empresa sin importar su rango o grado de confianza. |
| **Los sistemas de seguridad digital abarcan solo los equipos y software para evitar ciberataques y reducir los riesgos** | Concepto de intercambio de archivos, Data Sharing 3d - arte vectorial de Tridimensional libre de derechos |
| Verdadero(incorrecto)  Retroalimentación -=Además de la capacidad de los recursos tecnológicos, el grado de apropiación de las políticas y el cumplimento de estas por parte de los empleados define el éxito o fracaso del sistema de seguridad de la información. | **Falso (correcto)**.  Retroalimentación += Muy bien, existen otros elementos a tener en cuenta como, por ejemplo: el conocimiento y comportamiento de las personas de la organización, el sistema de seguridad que va más allá de lo tecnológico |
| **La certificación de la norma ISO 27001 solo tiene como objeto, cumplir con una formalidad ante las autoridades.** | concepto de iso. control de calidad. normas - iso 27001 fotografías e imágenes de stock |
| Verdadero(incorrecto)  Retroalimentación -=Es importante realizar la certificación porque la implementación trae mejoras y seguridad a la organización**.** | **Falso (correcto)**  Retroalimentación += Muy bien, la implementación de la norma garantiza un nivel de seguridad de la información muy superior en su organización. |

Retroalimentación General:

**Aprueba:** ¡**Muy bien**! Usted reconoce los activos tecnológicos, los riesgos a los que pueden estar expuestos y la normativa necesaria para prevenir y proteger la información de la empresa. ¡**Felicitaciones**!

**No aprueba:** ¡**Atención**! **Sus respuestas indican que debe** repasar los temas estudiados en el componente formativo para reconocer los activos tecnológicos, los riesgos a los que pueden estar expuestos y la normativa necesaria para prevenir y proteger la información de la empresa. ¡**Adelante**!

Material complementario

| Tipo de recurso | Material complementario | | |
| --- | --- | --- | --- |
| Tema | Referencia APA del material | tipo | Enlace |
| **Normativa: ISO 27001** | Procem Consultores (2018). ISO 27001 - Seguridad de la Información . <https://www.youtube.com/watch?v=BNdPQU32p2Y&ab_channel=ProcemConsultores> | Video | <https://www.youtube.com/watch?v=BNdPQU32p2Y&ab_channel=ProcemConsultores> |
| **Fundamentos de ciberseguridad** | Curso Introducción al Hacking & Penstesting (2020). Análisis de Vulnerabilidades. <https://www.youtube.com/watch?v=Rji6lKeZUvA> | Video | <https://www.youtube.com/watch?v=Rji6lKeZUvA> |
| **Activos de información** | Instituto Nacional de Tecnologías de la Información, España (2012). Activos de información. <https://www.youtube.com/watch?v=THnQ2FH7NtU> | Video | <https://www.youtube.com/watch?v=THnQ2FH7NtU> |
| **Fundamentos de ciberseguridad** | Rodríguez Cruz, D. (2020). Objetivos de la ciberseguridad y causas de los riesgos. <https://www.youtube.com/watch?v=0mqc4fde8y0> | Video | <https://www.youtube.com/watch?v=0mqc4fde8y0> |

Glosario

|  |  |
| --- | --- |
| Tipo de recurso | Glosario |
| Activo | hace referencia a un recurso propio de la empresa que genera y posee en sí mismo un valor, siendo importante para los procesos de esta. |
| Ciberataque | cualquier tipo de acción encaminada a causar daños a la información digital de una persona, empresa u otro tipo de organización. Por ejemplo, el robo de información privada, la alteración, destrucción o secuestro de información empresarial. |
| Credenciales de acceso | hace referencia al sistema utilizado para el acceso a carpetas, archivos, ambientes y espacios de la compañía. Las credenciales suelen ser usuario y contraseña, pin de seguridad, control biométrico entre otras. |
| Licencia | en informática, se refiere a las licencias como el acuerdo legal o contrato entre el desarrollador/proveedor del *software* y el usuario quien, mediante algún tipo de reconocimiento, puede usar dicho programa de manera legal y con derecho al soporte y acceso a las herramientas contratadas. |
| Norma | es una agrupación de conceptos, procedimientos y reglas sobre determinado tema o actividad, que han sido emitidos por un organismo reconocido con el objetivo de estandarizar, ordenar y definir la manera apropiada de hacer algo. |
| Política corporativa | conjunto de acciones implementadas por la empresa y exigidas a sus colaboradores para realizar las actividades relacionadas con el cumplimiento de los objetivos empresariales y buen funcionamiento de la misma. |
| Procedimiento | hace referencia al método o conjunto de actividades ordenadas para realizar determinada actividad. |
| Riesgo | situación que puede ocurrir en el sistema de información, desencadenando algún tipo de daño o perturbación en este. |
| Suplantación | acción de hacerse pasar o tomar responsabilidades de alguien más de manera fraudulenta, esto puede ocurrir, por ejemplo, cuando se ingresa sin autorización a las cuentas personales o laborales de alguien más, motivado principalmente por el hecho de obtener información sin autorización o consentimiento de su propietario. |
| Vulnerabilidad | son los puntos o aspectos del sistema que pueden ser susceptibles al sufrir algún tipo de incidente o ciberataque. |

**REFERENCIAS BIBLIOGRÁFICAS:**

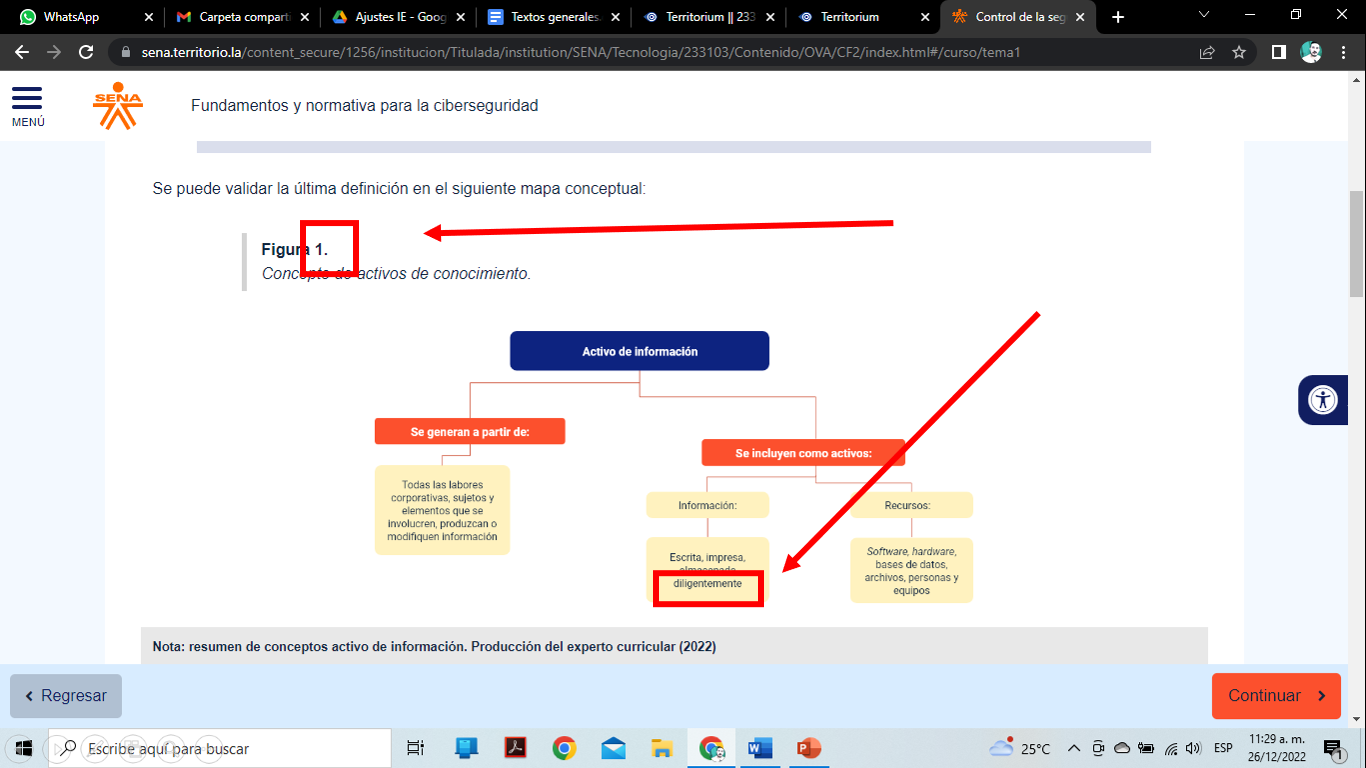
|  |  |
| --- | --- |
| **Tipo de recurso** | Bibliografía |
| Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad*.* Editorial CSIC Consejo Superior de Investigaciones Científicas. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/172144?page=7> | |
| Delitos informáticos en Colombia subieron un 17 % en el 2021: sepa cómo prevenirlos. (2021). Infobae. <https://www.infobae.com/america/colombia/2021/12/27/delitos-informaticos-en-colombia-subieron-un-17-en-el-2021-sepa-como-prevenirlos/#:~:text=%E2%80%9CSeg%C3%BAn%20cifras%20del%20Centro%20Cibern%C3%A9tico,capturas%E2%80%9D%2C%20revelaron%20las%20autoridades>. | |
| El ciberdelito creció 150% en el último año en el mundo. (2022). Portafolio. <https://www.portafolio.co/negocios/empresas/ciberdelito-crecio-150-en-el-ultimo-ano-en-el-mundo-566409> | |
| Giant, N. (2016). Ciber seguridad para la i-generación: usos y riesgos de las redes sociales y sus aplicaciones. Narcea Ediciones. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/46247?page=17> | |
| ISO 27001:2013 Guía de implantación para la seguridad de la información. (s.f.). Nga. <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf> . | |
| La cibercriminalidad costó más de u$s6 billones en 2021. (11 de mayo de 2022). Ámbito. <https://www.ambito.com/mundo/ciberseguridad/la-cibercriminalidad-costo-mas-us6-billones-2021-n5436916> | |
| Ministerio de tecnologías de la información y las telecomunicaciones [mintic].(2021). Política de Seguridad Digital. <https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital> | |
| Pérez-Montoro, M. (2009). Gestión del conocimiento.<http://glossarium.bitrum.unileon.es/Home/gestion-del-conocimiento-knowledge-management> | |
| Super intendencia de industria y comercio [SIC]. (2018). Metodología para la identificación, clasificación y valoración de activos de información. <https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Transparencia_y_acceso_a_la_informacion_publica/SC05-I03%20ACTIVOS%20DE%20INFORMACION%20(1)%20(1).doc> | |

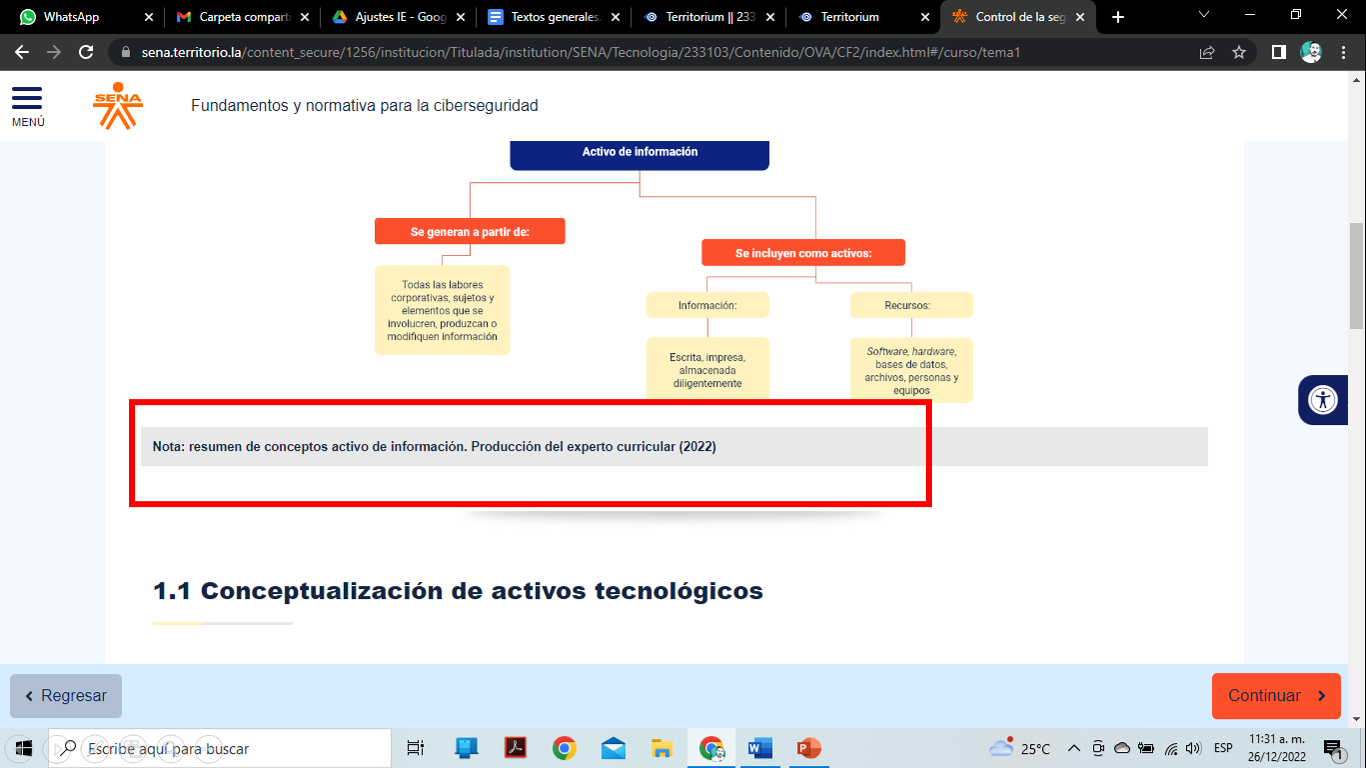
# **CONTROL DEL DOCUMENTO**

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

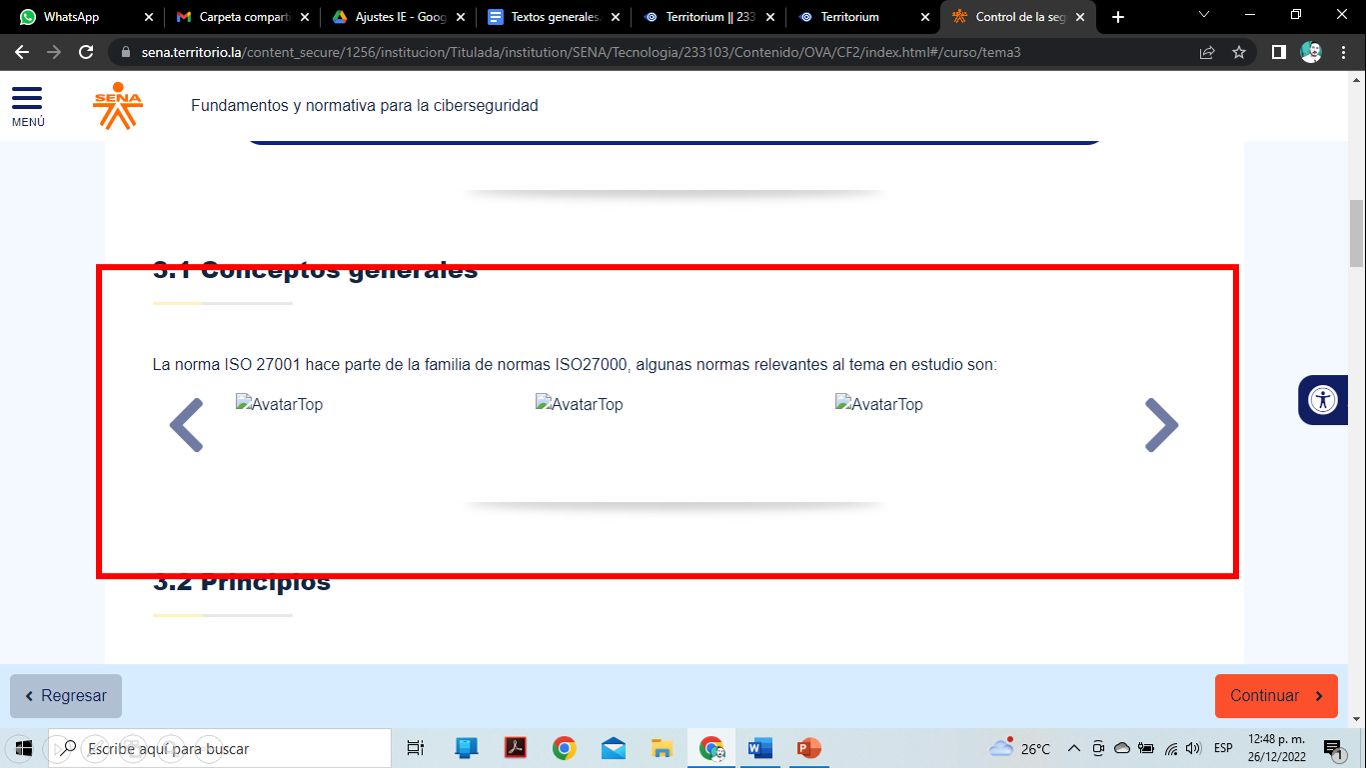
**CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)**

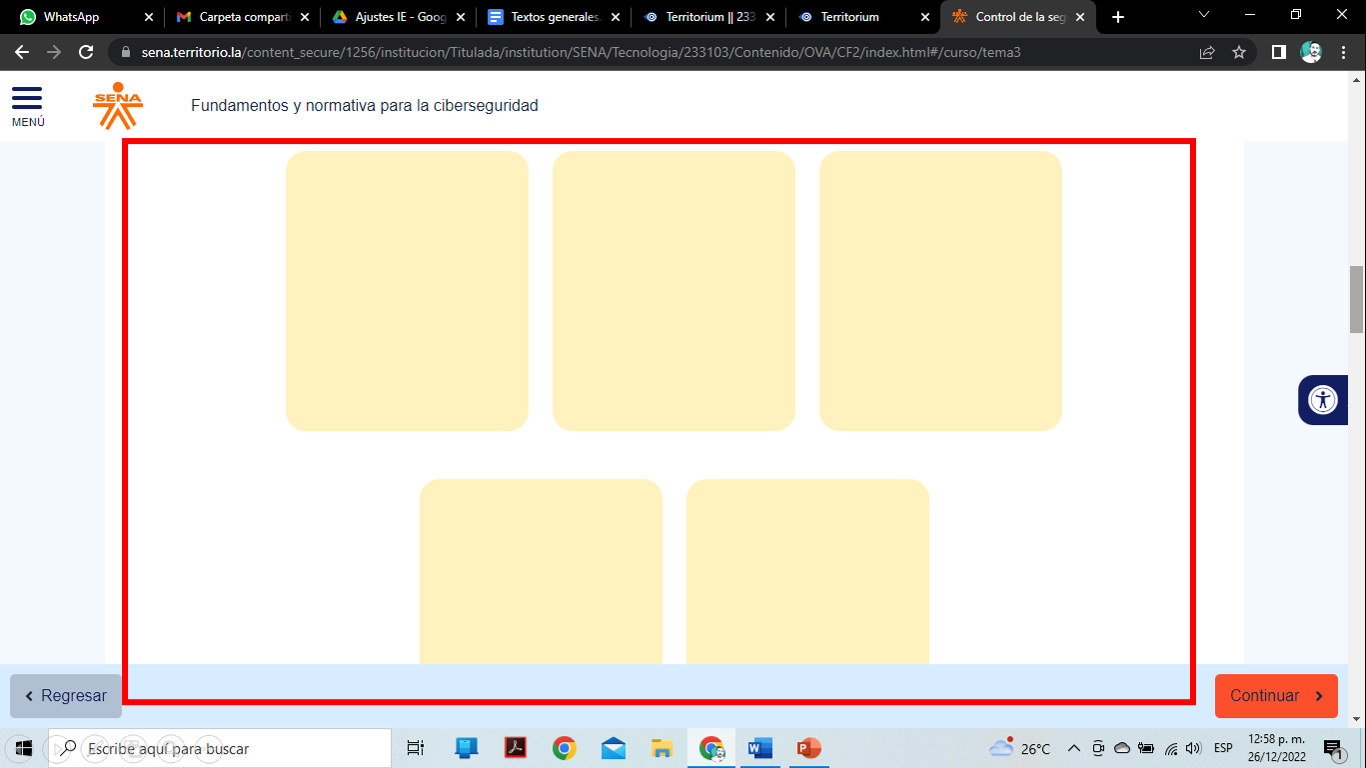
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del Cambio** |
| **Autor (es)** | Alejandra Mejía Restrepo | Corrector de textos | Innovate Education | Septiembre/2022 |  |

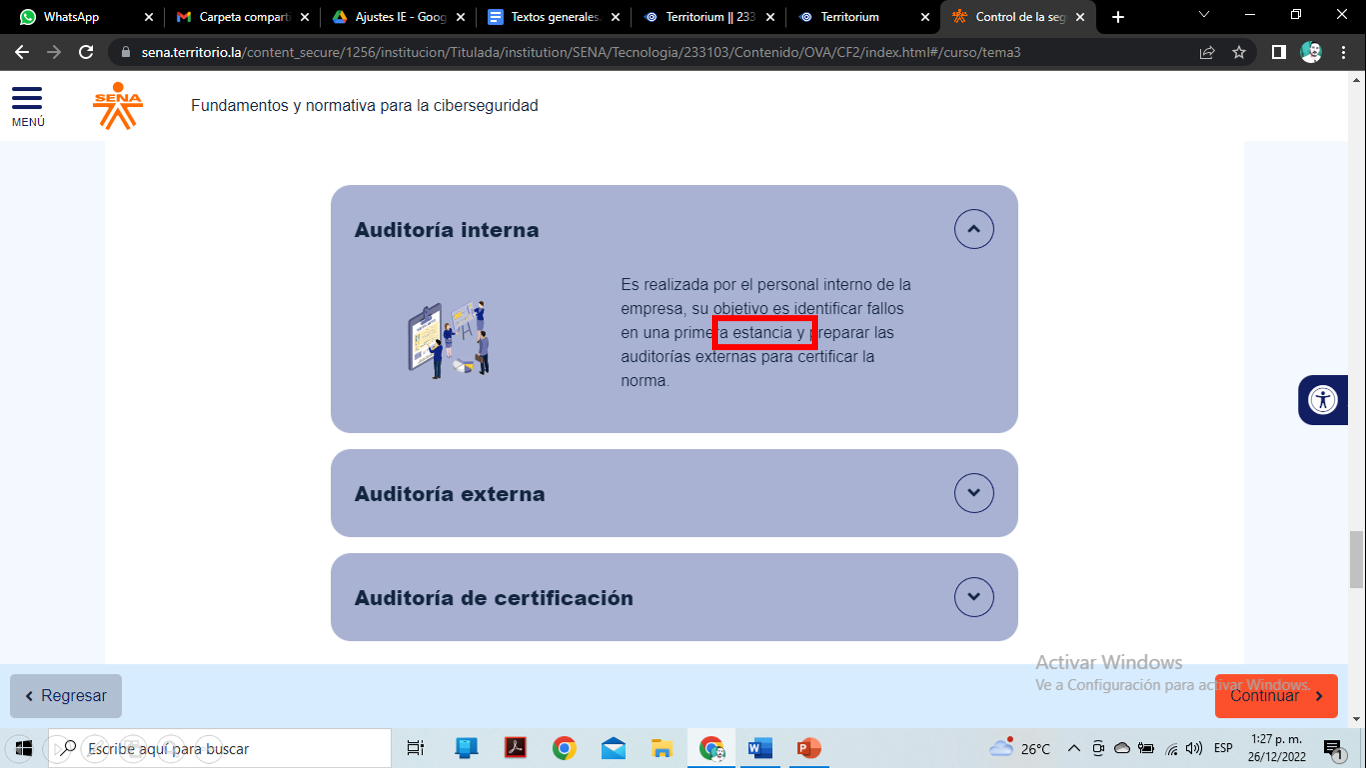


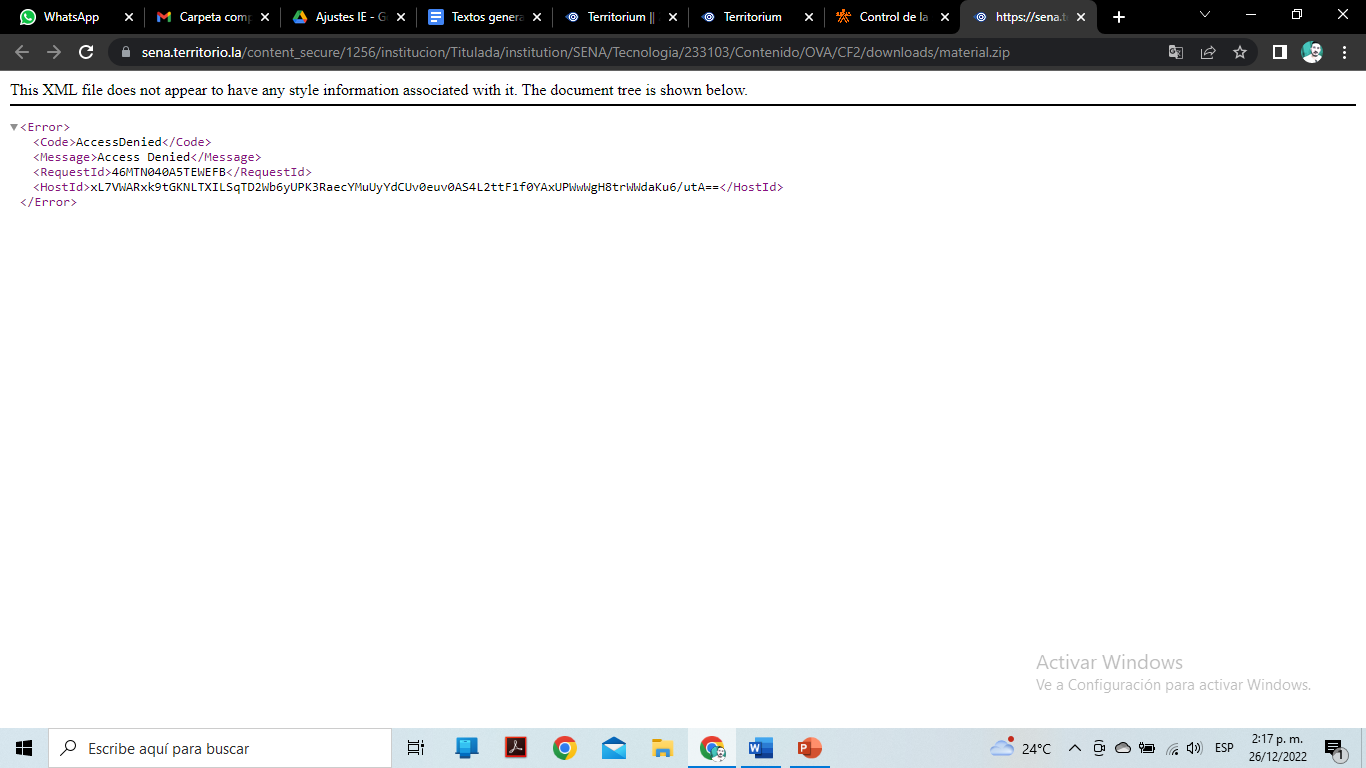












Texto

Descripción generada automáticamente