Guion para desarrollo de contenidos

**Datos de identificación del programa de formación**

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

| COMPETENCIA | 220501111. Controlar sistema de seguridad de la información de acuerdo con los procedimientos y su normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-02-Documentar incidentes de seguridad digital según criterios técnicos y marco de referencia |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 6 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Ciberseguridad y documentación de incidentes |
| BREVE DESCRIPCIÓN | Las empresas pueden verse expuestas a eventos e incidentes de seguridad que arriesgan los activos digitales, una forma de minimizar estos riesgos, es mediante buenas prácticas organizacionales, que conlleve a la creación de estándares y modelos de referencia que permitan documentar procesos dentro del sistema de gestión de seguridad de la información, realizar auditorías y trazabilidad de seguridad informática. (59) |
| PALABRAS CLAVE | Control de activos. Copia de seguridad. Informes. Sistemas de gestión. |

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

**TABLA DE CONTENIDOS**

**Introducción**

**1. Documentación de incidentes en la ciberseguridad**

1.1. Informes de operación de red de datos

1.2. Documentación de implementación

1.3. Informes de operación de herramientas de protección

**2. Reportes de incidente de la ciberseguridad**

2.1. Auditorias

2.2. Marco Jurídico y Marco Legal

2.3. Herramientas de gestión y manual de funcionamiento

2.4. Documentación de los procesos

**INTRODUCCIÓN**

| Cuadro de texto |
| --- |
| Estimado Aprendiz, bienvenido a este componente formativo que presenta los requerimientos asociados a la documentación de incidentes en la ciberseguridad, necesaria para registrar las operaciones de redes de datos y obtener la información para generar informes y reportes de operación en relación con las herramientas de protección y minimizar riesgos a los que puede verse expuesta la información.  Con diferentes contenidos audiovisuales puede apropiarse de la valiosa información que está aquí dispuesta, como parte del proceso de aprendizaje que adelanta y para continuar con los demás temas de estudio venideros. **Le invitamos a explorar el contenido y estudie a detalle todos los temas y al final realice la actividad de repaso.** |

**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** | Si desea conocer más información respecto a los puntos a tratar dentro del componente formativo le invitamos a ver el video de bienvenida, donde se explicará más a fondo los temas asociados a Ciberseguridad y documentación de incidentes**.**  **Documentación de incidentes** | | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración** | **Texto** |
| **1** | Simular personajes en oficina sentados frente a equipos de cómputo y con cara de preocupación, y alguien se acerca y pregunta, ¿nuevos incidentes? responden que sí, este personaje inicia la narración con la explicación. A manera de globos pueden aparecer imágenes o gif como los siguientes  gente de negocios trabajando juntos - personas preocupadas en la oficina fotografías e imágenes de stock    icono del documento plano - arte vectorial de Disco - Audio analógico libre de derechos | Música de fondo | Las empresas están expuestas a eventos e incidentes de seguridad que ponen en riesgo sus activos digitales, siendo necesario documentar o registrar las actividades de protección, generar reportes, informes de operación de red de datos, herramientas de protección y documentación de implementación según procedimiento técnico y marcos de referencia, también documentación asociada a procesos, normativas, auditorías y herramientas de gestión, que aportan a la ejecución de acciones para minimizar las amenazas que día a día evolucionan.  Para el cumplimiento de la normativa del gobierno digital es necesario implementar el modelo de seguridad que se desarrolla a través de cinco etapas:   * Diagnóstico. * Planificación * Implementación * Evaluación de desempeño y * Mejora continua   Cómo parte del proceso a seguir para garantizar la disponibilidad, integridad, transparencia y confidencialidad de los activos y datos digitales en las organizaciones, que a través de los registros y documentación permite el control, evaluación y seguimiento de la gestión. | Documentar eventos e incidentes de seguridad  Diagnóstico  Planificación  Implementación  Evaluación de desempeño  Mejora continua |
|  | Continuando con los personajes, y la narración, incluir vídeo con imágenes que ilustren lo que se está narrando, antivirus, backups, documentos leyes…  Vídeo  [https://www.istockphoto.com/es/v%C3%ADdeo/gr%C3%A1ficos-anal%C3%ADticos-financieros-y-de-colaboraci%C3%B3n-para-la-planificaci%C3%B3n-del-gm1395253401- 450431017](https://www.istockphoto.com/es/v%C3%ADdeo/gr%C3%A1ficos-anal%C3%ADticos-financieros-y-de-colaboraci%C3%B3n-para-la-planificaci%C3%B3n-del-gm1395253401-450431017)  concepto de software antivirus - antivirus fotografías e imágenes de stock  Personas revisando documentos  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de firma de contratos comerciales. documento corporativo. comprobación del acuerdo. protección de datos. términos y condiciones, política de privacidad - normativa  hermosos ingenieros informáticos masculinos y científicos crean una red neuronal en su estación de trabajo. office está lleno de pantallas que muestran representaciones 3d de redes neuronales. - monitoreo de red fotografías e imágenes de stock |  | La documentación debe cumplir con estándares y modelos de referencia para documentar los procesos dentro de un sistema de gestión de seguridad de la información.  A través, de auditorías y trazabilidad de seguridad informática se realizan verificaciones periódicas del estado de las plataformas de gestión de incidentes, antivirus, gestión y monitoreo de red, copias de seguridad y Backups.  Al recolectar la documentación, se obtiene evidencia digital, pero ésta debe ser tratada de acuerdo al marco jurídico, y al marco legal vigente en Colombia, regulados por las siguientes leyes: | Cumplir con estándares y modelos de referencia  Auditorías y trazabilidad  Evidencia digital  Normas y Leyes |
|  | empresario tocando el icono del equilibrio de la justicia. concepto de asesoramiento jurídico, derecho y defensa. - leyes fotografías e imágenes de stock |  | * Ley 1273 de 2009: Que modifica el código penal y crea como bien jurídico tutelado la protección de la información y de los datos. * Ley 1581 de 2012: De los Principios y disposiciones que definen los derechos sobre los datos personales y denuncia de las violaciones de seguridad. * Decreto 1377 de 2012: Que Reglamentó aspectos relacionados con la titularidad del uso de la información para el tratamiento de los datos personales. | Ley 1273 de 2009  Ley 1581 de 2012  Decreto 1377 de 2012 |
|  | Cuando el narrador mencione cada momento, se puede poner en relieve cada uno y luego las características.  **Momentos de la política de Gobierno Digital**    Gráfico 1. Gobierno Digital. Fuente: MANUAL DE GOBIERNO DIGITAL, 2018. Recuperado de: Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) |  | Con la vigencia de este marco legal, y después de varios años se logró implementar la estrategia de Gobierno en Línea, cómo se refleja en este gráfico. Las políticas de gobierno digital se concentran en cuatro momentos, a través, de los cuales las entidades públicas han logrado grandes avances en materia de eficiencia administrativa, participación, servicios ciudadanos y medios electrónicos; sin embargo, la evolución continua del país y de la sociedad hacia la digitalización de la economía y la información, exigen el desarrollo de procesos hacia la transformación digital, dentro de los que está la seguridad digital. | Estrategia de Gobierno en Línea  Momentos de la política de Gobierno Digital |
|  | Hombre de negocios que utiliza un concepto de administración de computadoras para documentos, base de datos de documentación en línea y sistema / software de almacenamiento de archivos digitales, mantenimiento de registros, tecnología de base de datos, - Foto de stock de Tecnología libre de derechos  Gráfico 2. Hombre de negocios que utiliza un concepto de administración de computadoras para documentos, base de datos de documentación en línea y sistema / software de almacenamiento de archivos digitales, mantenimiento de registros, tecnología de base de datos. Fuente: istockphoto, 2021. Recuperado de  Estadísticas del concepto de negocio. Gráfico financiero. Planificación financiera. análisis de datos. Estrategia de gestión. - Foto de stock de Informe libre de derechos  Gráfico 3. Estadísticas del concepto de negocio. Gráfico financiero. Planificación financiera. análisis de datos. Estrategia de gestión. Fuente: istockphoto, 2021. Recuperado de |  | De este modo, y para realizar una gestión eficiente en el tratamiento de la información de acuerdo a los requerimientos de las auditorías, se necesita el uso de herramientas de gestión como plataformas colaborativas, y de gestión documental. Éstas herramientas deben contar con una guía de operación con especificaciones técnicas para ayudar a cualquier persona que se enfrente por primera vez a su uso.  Le invito a que inicie con el estudio de este componente de formación, explorando cada recurso, y al finalizar desarrolle la actividad didáctica de repaso. (497) | Herramientas de gestión  -Plataformas colaborativas  -Plataformas de gestión documental |
| **Nombre del archivo** | **233103\_CF06\_v1.mp3** | | | | |

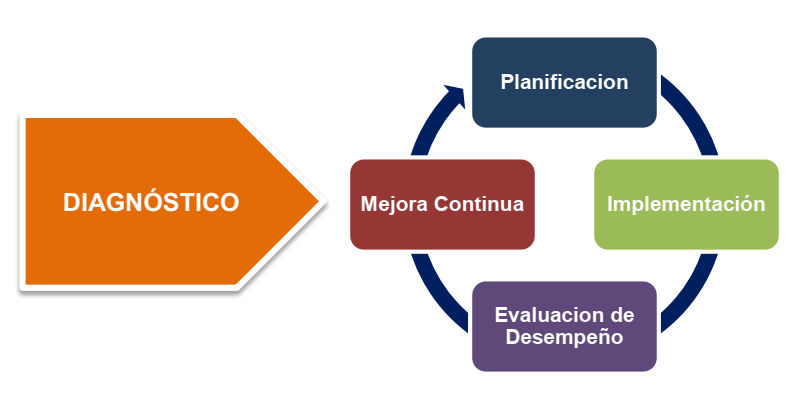
**DESARROLLO DE CONTENIDO**

**1.** **Documentación de incidentes en la Ciberseguridad**

| Tipo de recurso | Cajón de texto |
| --- | --- |
| Los procesos que permiten gestionar y dar tratamiento a los incidentes de la ciberseguridad se rigen bajo la familia de las normas ISO/IEC 27000. Estas normas describen lineamientos para el seguimiento de eventos, incidentes y acciones que lleguen a impactar en el desempeño de los sistemas de seguridad de la información en las empresas.  En Colombia, está contemplado dentro del marco de gobierno digital el Modelo de Seguridad y Privacidad de la Información – MSPI. Este modelo está basado en un ciclo de operación que incluye 5 fases:   * Diagnóstico * Planificación * Implementación * Evaluación de desempeño * Mejora continua   Gráfico 4. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información. Fuente: MinTic, 2016. Recuperado de: Modelo de Seguridad y Privacidad de la Información | |

**Figura 1**

*Ciclo de operación del Modelo de Seguridad y Privacidad de la Información*



Nota: tomada y adaptada de Ministerio de las TIC (2016). Modelo de Seguridad y Privacidad de la Información.

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Estas fases, logran que las entidades que implementan el MSPI gestionen de manera adecuada la seguridad y privacidad de los activos digitales, de este modo, la Estrategia de Gobierno en línea, permite centrarse en los componentes de Tecnología de la Información y Comunicaciones TIC para gestionar aportes que incluyen la formulación, gestión e implementación de un modelo de seguridad enfocado en salvaguardar la disponibilidad, integridad, transparencia y confidencialidad de los activos y datos digitales, mediante buenas prácticas de documentación de eventos e incidentes, dando cumplimiento a los objetivos y misión de la entidad.  erp, concepto de gestión documental. hombre de negocios que trabaja con una computadora portátil con iconos en la pantalla virtual y fondo borroso de la oficina. - informes fotografías e imágenes de stock    Los sistemas de gestión sostenibles adoptados por las entidades, generan la percepción y aceptación de un estado más transparente, abierto al público, participativo y colaborativo, garantizando que la información entregada al ciudadano cuenta con controles y criterios de seguridad, documentado cada incidente que altere o modifique algún dato dentro del universo de información almacenada. | |

* 1. **Informes de operación de red de datos**

| Tipo de recurso | Cajón de texto |
| --- | --- |
| De acuerdo a las etapas del MSPI en su fase de diagnóstico se identifica la operatividad de la red de datos según procedimientos técnicos y marcos de referencia; Es así que se describe el estado de la entidad, el nivel de madurez y el levantamiento de información, teniendo en cuenta los requerimientos, metas y resultados.  En esta etapa, al generar los informes de operación de la red de datos, se debe describir las metas, los resultados e instrumentos utilizados, tal como se describe en la siguiente en la figura 2 y la tabla 1: | |

**Figura 2**

*Fase de diagnóstico MSPI.*



Nota: tomada y adaptada de Ministerio TIC (2016). Modelo de Seguridad y Privacidad de la Información

**Tabla 1.**

*Fase de diagnóstico*

| **METAS** | **RESULTADOS** | **INSTRUMENTOS MSPI** |
| --- | --- | --- |
| Establecer el estado actual de la entidad en la gestión de seguridad y privacidad de la información – SPI | Herramienta diligenciada y documentada | Herramienta de diagnóstico |
| Identificar el nivel de madurez de SPI en la Entidad | Herramienta diligenciada y nivel de madurez identificado | Herramienta de diagnóstico |
| Identificar vulnerabilidades técnicas y administrativas, las cuales serán los insumos para la planificación | Informe con los hallazgos obtenidos de las pruebas de vulnerabilidad | Herramienta de diagnóstico |

Nota. Esta tabla describe las metas, resultados e instrumentos de la fase de diagnóstico del MSPI. Tomada y adaptada de Ministerio TIC (2016). Modelo de Seguridad y Privacidad de la Información

| **Tipo de recurso** | Slider pasos | |
| --- | --- | --- |
| **Introducción** | Para el desarrollo eficiente de esta fase, las entidades necesitan seguir estos pasos: | |
| **Slide 1** | Recolectar la información a través de la herramienta de diagnóstico | especialista femenina en servidores de ti de pie en el centro de datos. vea desde rack server cabinet con iconos de interfaz de usuario de cloud server y visualización en primer plano. - diagnostico ciberseguridad fotografías e imágenes de stock |
| **Slide 2** | Implementar las pruebas de efectividad | empresario tocando tablero de dardos virtuales con flecha, concepto objetivo de logro empresarial. - pruebas efectividad fotografías e imágenes de stock |
| **Slide 3** | Documentar el resultado del diagnóstico | bombilla iluminada, concepto de marca idea de explotación de la mano de la mujer. - pruebas efectividad fotografías e imágenes de stock |
| **Slide 4** | Determinar el nivel de madurez | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de edades de la mujer - madurez |
| **Slide 5** | Éstos resultados necesitan ser revisados y divulgados por todas las personas que intervienen en el proceso para iniciar con la siguiente fase. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ideación, lluvia de ideas para reunir nuevas ideas, discusión efectiva en reuniones, miembros del equipo descubren soluciones, concepto scrum, lluvia de ideas de personas de negocios con notas adhesivas combinadas con una idea de bombilla brillante. - resultados |

| Tipo de recurso | Cajón de texto |
| --- | --- |
| En la **fase de planificación**, se utilizan como insumos los resultados de la etapa de diagnóstico para elaborar los informes con el método de SPI, con el objetivo de determinar los procesos que se deben implementar a nivel de SPI, mediante la estructura de gestión del riesgo en la operación de la red de datos.  La Entidad es la encargada de limitar los procesos a ejecutar para la implementación de SPI. Estos procesos deben ser universales y abarcar todos los departamentos de la entidad; Es preciso que el alcance y limitantes impacten el cumplimiento de los objetivos, protegiendo la calidad de la información y los servicios, sobre todo la documentación de acuerdo a los informes de la operatividad en la red de datos.  ingeniero técnico industrial de trabajo y control robótica con monitoreo sistema icono y software industria conexión de red en tableta. máquina de brazo de robot ai, inteligencia artificial, automatización en fábrica de smart en fondo digital azul, i - implementacion sistemas fotografías e imágenes de stock | |

| **Tipo de recurso** | Acordeón tipo 1 |
| --- | --- |
| **Introducción** | A continuación, se detalla el proceso de la etapa de planificación y las partes que debe contener un informe de gestión, junto con sus metas, resultados e instrumentos para el MSPI en una entidad. |
| Como se puede observar, la fase de planificación contiene 4 subprocesos: Contexto, liderazgo, planeación y soporte.  **Figura 3**  *Fase de planificación MSPI*    Nota: tomada cómo referencia del Ministerio TIC,(2016). Recuperado de: Modelo de Seguridad y Privacidad de la Información | |
| **Contexto:**  Se debe conocer, investigar y hallar oportunidades de mejora dentro del MSPI, para determinar los alcances del mismo. | |
| **Liderazgo:**  En el marco de apropiación del MSPI, los líderes y directores de las entidades deben propender porque todos los funcionarios acaten y sientan el compromiso de dar fiel cumplimiento a la normatividad, asignando roles y responsabilidades en cada uno de los aspectos a tratar. | |
| **Planeación:**  Plantear acciones y objetivos, de tal manera que se cree la hoja de ruta para abordaje de eventos e incidentes. | |
| **Soporte:**  Documentar la entrega de recursos y competencias a cada área de manera oficial, mediante sensibilizaciones y comunicaciones. | |

**1.2. Documentación de implementación**

| **Tipo de recurso** | Acordeón tipo 1 |
| --- | --- |
| **Introducción** | En este ítem se aborda la etapa de implementación del MSPI, donde se logrará llevar acabo la implementación de lo planificado en los informes de operación de red de datos. Esta etapa contiene 3 subprocesos como son: Control y planeación operacional, plan de tratamiento de riesgos de seguridad y privacidad de la información, y la definición de indicadores de gestión. |
| **Figura 4**  *Fase de implementación MSPI*    Nota: tomado de MinTic, 2016. Recuperado de: Modelo de Seguridad y Privacidad de la Información | |
| **Control y planeación operacional:**  La entidad planifica, implementa y controla todos los procesos indispensables que permitan cumplir con todas las condiciones necesarias de SPI. Es indispensable, que toda esta información sea documentada para llevar un control de acciones en búsqueda de la mitigación de riesgos que puedan presentarse. | |
| **Plan de tratamiento de riesgos de SPI:**  Es indispensable la implementación del plan de tratamiento de riesgos, en donde se debe identificar los controles aplicar para que éstos lleguen a un nivel aceptable. | |
| **Definición de indicadores de gestión:** La definición de indicadores permiten la medición de eficiencia y efectividad en las acciones implementadas en SPI. Los indicadores permiten medir eficiencia, efectividad, y mejora continua. | |

| Tipo de recurso | Cajón de texto |
| --- | --- |
| Por otro lado, es importante definir las actividades a realizar para la migración de los protocolos IPv4 a IPv6, cabe recordad que las Ipv son las conexiones de internet, siendo la IPv4 más antigua y vulnerable, a partir del 2020 se migró a la IPv6. En esta fase se realizan actividades de direccionamiento, diseño, montaje, ejecución y corrección de pruebas, activación de políticas de SPI, validación de funcionalidad, a continuación, se describen metas, entregables e instrumentos para la migración de Ipv4 a Ipv6. | |

**Tabla 3.**

*Migración Ipv4-Ipv6*

| **METAS** | **RESULTADOS** | **INSTRUMENTOS MSPI** |
| --- | --- | --- |
| Implementar la estrategia de migración IPv4 a IPv6. | Informe para implementar la estrategia de migración de IPv4 a IPv6 | Guía Transición de IPv4 a IPv6 para Colombia |

*Nota.* Esta tabla describe las metas, resultados e instrumentos de la migración de Ipv4 a Ipv6

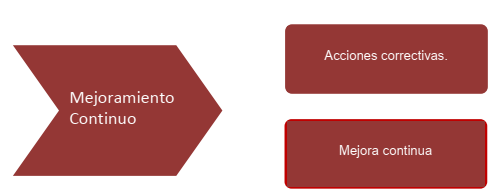
**1.3. Informes de operación de herramientas de protección**

| **Tipo de recurso** | Tarjetas Conectadas |
| --- | --- |
| **Introducción** | Existen herramientas de protección que permiten la operación continua de la entidad, es indispensable documentar cada etapa del proceso y generar informes, este aspecto hace parte del MSPI en las etapas de evaluación de desempeño y mejora continua.  En la etapa de evaluación de desempeño se realiza el seguimiento al MSPI, de acuerdo a los resultados obtenidos en la etapa de implementación. Este proceso permite verificar la eficiencia de todas las acciones que se implementan. |
| **Figura 5**  *Fase de evaluación de desempeño MSPI*    Nota: tomado de MinTic, 2016. Recuperado de: Modelo de Seguridad y Privacidad de la Información  Como se puede observar, la etapa de evaluación de desempeño contiene 3 fases a su vez actividades, metas y resultados que permite la consolidación de los indicadores. | |
|  | **Actividades**   * Revisar actividad de controles. * Revisar evaluación por nivel de riesgo. * Hacer seguimiento a las actividades ejecutadas. * Hacer seguimiento a la implementación del MSPI. * Hacer seguimiento a los registros. * Medir indicadores de gestión. * Hacer revisión a los planes de mejora. * Especificar frecuencia, métodos, y responsables. * Planificar y elaborar informes. * Conservar información documentada en los informes. |
|  | **Metas**   * Informe plan de revisión y seguimiento * Informe de auditorías |
|  | **Resultados**   * Documento con plan de seguimiento * Documento con el plan de auditorías |

| Tipo de recurso | Cajón de texto |
| --- | --- |
| Para finalizar con las etapas, se procede con la de mejora continua que consolida los resultados de la fase de evaluación de desempeño, en búsqueda del plan de mejoramiento continuo de SPI, ejecutando acciones previas que mitiguen los efectos de los incidentes que se presenten. | |

**Figura 6**

*Fase de mejoramiento continuo MSPI.*



Nota: tomado como referencia de MinTic, 2016. Recuperado de: Modelo de Seguridad y Privacidad de la Información

| Tipo de recurso | Cajón de texto |
| --- | --- |
| Como se puede observar, la etapa de mejoramiento continuo consta de 2 fases que son: Acciones correctivas y mejora continua; cada una de estas fases contiene metas, resultados e instrumentos. | |

**Tabla 4.**

*Mejoramiento continuo*

| **METAS** | **RESULTADOS** | **INSTRUMENTOS MSPI** |
| --- | --- | --- |
| Realizar el plan de mejora.  Analizar los resultados del seguimiento.  Analizar los resultados de las auditorías. | Informe con plan de mejora  Informe con plan de divulgación | Guía de mejora continua |

*Nota.* Esta tabla describe las metas, resultados e instrumentos de la fase de mejoramiento continuo. tomado como referencia de MinTic, 2016. Recuperado de: Modelo de Seguridad y Privacidad de la Información

**2. Reportes de incidente de la ciberseguridad**

| **Tipo de recurso** | Acordeón tipo 2 |
| --- | --- |
| **Introducción** | Los reportes de incidentes permiten identificar, evaluar, y responder a eventos del sistema de información. Éstos manejan un nivel de madurez que busca establecer criterios de valoración y determina el estado de la SI en las entidades. Existen 6 niveles de madurez y abarca desde la inexistencia hasta la optimización. |
| **Figura 7**  *Nivel de madurez*    Nota: tomado de MinTic, (2016). Recuperado de: Modelo de Seguridad y Privacidad de la Información | |
| **Inexistencia**   * No se implementa control de infraestructura de TI, física, y recursos humanos. * No se reconoce la información como un activo digital sensible e importante. | |
| **Inicio**   * Se hace una aproximación a las debilidades y falencias de SI. * Los incidentes son tratados de manera reactiva. * Se detecta la necesidad de implementar el MSPI. | |
| **Repetición**   * Se identifica y clasifica a manera general los activos de información. * Se crea la cultura de conciencia de SI entre los funcionarios. * Todo lo relacionado con SPI es tratado en comités de gestión. * La entidad hace la migración de Ipv4 a Ipv6 y cuenta con una planeación. | |
| **Definición**   * Se realiza el diagnóstico permitiendo saber el estado en SI. * Se determinan objetivos, acciones, alcances de SI. * Se establece políticas, procedimientos, roles y responsabilidades de Si y se divulgan en toda la entidad. * Se realiza inventario de activos de información. * Se implementa un plan de tratamiento de riesgo. * La entidad hace la migración de Ipv4 a Ipv6 y documenta el plan de transición. | |
| **Administración**   * Revisión y monitoreo periódico de activos de información. * Uso de indicadores KPI para cumplimiento de políticas de SPI. * Evaluar efectividad de acciones que permita disminuir incidentes, evitando repeticiones a futuro. * Prueba constante de uso Ipv6. | |
| **Optimización**   * La seguridad como valor agregado para cumplimento de metas en la entidad. * La Información tiene un valor único y es inalterable. * La información cumple con los criterios de transparencia, claridad, oportunidad, integridad y disponibilidad. * Uso de indicadores para mejora de compromisos misionales. * Se genera tráfico Ipv6. | |

**2.1. Auditorias**

| Tipo de recurso | Cajón de texto |
| --- | --- |
| En muchas oportunidades no se aprecia el alto grado de exposición a vulnerabilidades en ciberseguridad que enfrentan las entidades día tras día, es por ello, que lo más idóneo es realizar una auditoría. Estas acciones que van enmarcadas a través de buenas prácticas normalizadas por ISO 27000, permite detectar, enlistar y documentar aquellas incidencias y vulnerabilidades en la infraestructura TIC de la entidad. Los objetivos de las auditorías son:   * Analizar situación actual de la entidad y rendimiento de la productividad. * Realizar una propuesta de seguridad física perimetral. * Analizar y planear la mejora técnica de la red interna. * Analizar el hardware, software, y comunicaciones que ayude a generar las políticas de actualización y vulnerabilidades de la entidad. * Enlistar las recomendaciones de mejora continua y buenas prácticas en la configuración y acceso al hardware. * Realizar pruebas de huella externa (Fase External Footprinting - FEF). * Realizar pruebas de ficheros remotos RFI. * Probar los servidores, firewall y PC’s, mediante escáner y pruebas manuales de autenticación. * Analizar red inalámbrica (Wireless) con el fin de saber, que operación realiza una persona que acceda a esta red. * Realizar un documento que describa las medidas a implementar y las acciones preventivas de mantenimiento en hardware y software.   gestión de la calidad con qa (aseguramiento), qc (control) y mejora. concepto de normalización y certificación. cumplimiento de normativas y estándares. gerente o auditor que trabaja en la computadora. - auditoria fotografías e imágenes de stock | |

| **Tipo de recurso** | Slider Hitos/ Línea de tiempo horizontal | |
| --- | --- | --- |
| **Introducción** | El objetivo de las auditorías no es el de realizar actividades puntuales, sino acciones continuas que logran disminuir, minimizar y bloquear las amenazas latentes que están en continua transformación. De este modo, la entidad estaría preparada para actuar o prevenir consecuencias que se puedan presentar y así mejorar continuamente la seguridad y privacidad de los datos. Entre los tipos de auditorías más populares encontramos:  Un hombre de negocios que calcula la probabilidad de riesgos en la protección de la seguridad cibernética utilizando la calculadora. Iconos de holograma de candado sobre el escritorio de trabajo. Ropa formal. - Foto de stock de Auditoría libre de derechos | |
| **Hacking ético** | Se realiza una serie de ciberataques para detectar la vulnerabilidad de la entidad. | gerente técnico industrial ingeniero de trabajo y control de la robótica con el software del sistema de monitoreo e icono de conexión de red en la tableta. ai, inteligencia artificial, brazo robótico de automatización - implementacion sistemas fotografías e imágenes de stock |
| **Auditoría web** | El objetivo es detectar la seguridad del servidor y la página web de la entidad. | joven concepto de ingeniero femal e. gui (interfaz gráfica de usuario). - implementacion sistemas fotografías e imágenes de stock |
| **Auditoría de la red** | Actualizar el firmware de los sistemas operativos y dispositivos. Revisar proceso de conexión a internet y mapa de conexiones de la entidad. | hermosos ingenieros informáticos masculinos y científicos crean una red neuronal en su estación de trabajo. office está lleno de pantallas que muestran representaciones 3d de redes neuronales. - implementacion sistemas fotografías e imágenes de stock |
| **Auditoría de código** | Realizar pruebas de código a las App que se usan en la entidad. | concepto de negocio y tecnología. - implementacion sistemas fotografías e imágenes de stock |
| **Auditoría de código** | Realizar pruebas de conexión y navegabilidad de los dispositivos conectados a la red inalámbrica. | concepto de transporte y logística, gerente e ingeniero de verificación y control de la distribución de la red logística y datos en tableta para la exportación logística de importación en el fondo de la autopista - implementacion sistemas fotografías e imágenes de stock |

| **Tipo de recurso** | Infografía estática |
| --- | --- |
| **Texto introductorio** | Sin importar el tamaño de la entidad, todas requieren de auditorías de ciberseguridad; Mantener operativa y segura la infraestructura tecnológica, genera confianza en los usuarios y elevan los niveles de calidad y productividad al interior de ésta. A continuación, de presentan las acciones que no pueden faltar en las auditorias de ciberseguridad: |
| **Imagen**    **Acciones de auditoría en Ciberseguridad**   * Analizar el software instalado en los equipos de la entidad. * Comprobar y plantear las posibles amenazas, vulnerabilidades, acciones y medidas como procedimiento de buena práctica. * Verificar si la entidad cumple con todos los aspectos del procedimiento que se enmarca en los estándares de calidad. * Implementar las acciones de mejora que se estipulen como cumplimiento de calidad. * Analizar dispositivos, sistemas operativos, redes alámbricas e inalámbricas, y App.   <https://img.freepik.com/vector-gratis/plantilla-infografia-linea-tiempo-plana_23-2148906597.jpg?w=996&t=st=1661953013~exp=1661953613~hmac=b0167760f71799005bb5b2bb69e7c645cf3e3b216affdd13faa3b2ccec65ee5d>  iconos: <https://media.istockphoto.com/vectors/user-experience-icon-set-vector-id1096480126?k=20&m=1096480126&s=612x612&w=0&h=E8kSy-A-OEGp6dmBouw2wJ7q0duAU3IPHGd9zMJEXbg>= | |
| **Código de la imagen** | **Cod.Imagen:** 233103\_CF6\_i024 |

| **Tipo de recurso** | Infografía estática |
| --- | --- |
| **Texto introductorio** | En conclusión, una auditoría en ciberseguridad sirve para tener conocimiento e identificar algunos factores al interior de la entidad, tales como: |
| **Imagen**     * **Exposición a las amenazas:** Grado de exposición a las amenazas. * **Inconvenientes con la información:** Inconvenientes que impiden garantizar que la información sea integra, transparente, confidencial y disponible. * **Eficiencia de software:** Eficiencia de los sistemas y software instalados. * **Seguridad de las contraseñas:** Seguridad de las contraseñas de los funcionarios de la entidad. * **Seguridad del sitio web:** Seguridad de la red y sitio web. * **Cumplimiento de normas:** Cumplimiento de las normas, políticas y manuales de ciberseguridad.   <https://img.freepik.com/vector-gratis/infografia-valores-fundamentales-planos-dibujados-mano_23-2149065129.jpg?w=740&t=st=1661954430~exp=1661955030~hmac=19e0e995326e83118bcc635e08b52108cdfbe011e5f2f483490b309aecdab560>  iconos: <https://media.istockphoto.com/vectors/line-business-management-icons-vector-id990288238?k=20&m=990288238&s=612x612&w=0&h=x6i4Zz6u8duiAF7nv6Mt8hpALj0ObDJy8MLZMdcr0LA>=  <https://media.istockphoto.com/vectors/account-security-thin-line-vector-icon-set-pixel-perfect-editable-vector-id1339454542?k=20&m=1339454542&s=612x612&w=0&h=Wbq47hTEc4u2e1deStIejtu_ND7PPVCjxPwncq_CLtQ>= | |
| **Código de la imagen** | **Cod.Imagen:** 233103\_CF6\_i025 |

**2.2. Marco Jurídico y Marco Legal**

| **Tipo de recurso** | Acordeón tipo 2 |
| --- | --- |
| **Introducción** | En la actualidad, existen diversos instrumentos Normativos de Ciberseguridad, con los cuales, el gobierno busca regular y controlar los ciberataques y los ciberdelincuentes; Entre los decretos, leyes y artículos se destacan: |
| ley de normas de cumplimiento e interfaz gráfica de regulación para la política de calidad empresarial - normas leyes fotografías e imágenes de stock  **Cod.Imagen:** 233103\_CF6\_i026  <https://media.istockphoto.com/photos/compliance-rule-law-and-regulation-graphic-interface-for-business-picture-id1255773628?k=20&m=1255773628&s=612x612&w=0&h=QBmMXmfMzLYZFcnEkkcsSP1gx-YgBen0sr1UA76hJMk>=  **Imagen:** Construya aquí el código de la imagen | |
| **CONPES 3701 DE 2011** – Lineamientos de política para la Ciberseguridad y Ciberdefensa. En este documento se generan los lineamientos que permiten desarrollar estrategias del orden nacional para contrarrestar las amenazas informáticas. | |
| **Ley 527 de 1999** – Validez jurídica y probatoria de la información electrónica. Ley donde se reglamenta el acceso y uso a los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. | |
| **Ley 594 de 2000** – Ley General de Archivos. El objetivo de esta ley es establecer las reglas y principios generales que regulan la función archivística del Estado. | |
| **Ley 679 de 2001** – Prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores. El objeto de esta ley es la protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio. | |
| **Ley 962 de 2005** – Simplificación y Racionalización de Trámites y procedimientos administrativos. Esta ley permite facilitar las relaciones de los particulares con la Administración Pública. | |
| **Ley 1150 de 2007** – Seguridad de la información en contratación pública. El objeto de la presente ley es la modificación en la Ley 80 de 1993, y dictar otras disposiciones generales aplicables a toda contratación con recursos públicos. | |
| **Ley 1266 de 2008** – Habeas data. Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos. | |
| **Ley 1273 de 2009** – Protección de información de los datos. Crea el marco contra los atentados a la confidencialidad, integridad y disponibilidad de los datos. | |
| **Ley 1341 de 2009** – Principios y conceptos sobre la sociedad de la información y la organización de las TIC. Determina el marco general para la formulación de las políticas públicas que regirán el sector de las TIC y su ordenamiento general. | |
| **Ley 1437 de 2011** – Procedimiento Administrativo y de lo Contencioso Administrativo. Proteger y garantizar los derechos y libertades de las personas, la primacía de los intereses generales, la sujeción de las autoridades a la Constitución y demás preceptos del ordenamiento jurídico. | |
| **Ley 1480 de 2011** – Estatuto del consumidor. Por la cual se protege al consumidor de medios o mercado electrónico. | |
| **Decreto Ley 019 de 2012** – Racionalizar trámites a través de medios electrónicos. Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. | |
| **Ley 1581 de 2012** – Protección de datos personales. Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos. | |
| **Ley 1712 de 2014** – Transparencia y derecho al acceso a la información pública nacional. Regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. | |
| **Decreto 2364 de 2012** – Firma electrónica. Representa un medio de identificación electrónico flexible y tecnológicamente neutro que se adecúa a las necesidades de la sociedad. | |
| **Decreto 2609 de 2012** – Expediente electrónico. Fortalecer de los archivos públicos del país, para garantizar la eficacia de la gestión del Estado y la conservación del patrimonio documental. | |
| **Decreto 2693 de 2012** – Gobierno en línea. Lineamientos, plazos y términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente, más transparente y participativo. | |
| **Decreto 1377 de 2013** – Protección de datos. Reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. | |
| **Decreto 1510 de 2013** – Sistema de compras y contratación Pública. Las Entidades Estatales deben procurar el logro de los objetivos del sistema de compras y contratación pública definidos por Colombia Compra Eficiente. | |
| **Decreto 333 de 2014** – Entidades de certificación. Definir el régimen de acreditación de las entidades de certificación | |

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Para ampliar la información y a manera de ejemplo, se puede referir a los anexos:  Ver Anexo 1: MARCO JURÍDICO CIBERSEGURIDAD PONAL.  Ver Anexo 2: Convenio sobre la Ciberdelincuencia - LEY 1928 DE JULIO 24 DE 2018 | |

**2.3. Herramientas de gestión y manual de funcionamiento**

| **Tipo**  **de recurso** | Pestañas o tabs horizontales | |
| --- | --- | --- |
| **Introducción** | Para que los sistemas no sufran consecuencias tras los ataques de ciberseguridad, es importante contar con herramientas de protección y, además, que los encargados de éstas cuenten con las habilidades y conocimientos para su óptimo funcionamiento: | |
| Software  antivirus | Estos programas permiten contar con medidas de protección efectivas cuando el equipo se encuentre expuestos a software malicioso o cualquier otro tipo de malware; Estos programas ofrecen la oportunidad de eliminarlo por completo o poner en estado de cuarentena.  Para conocer la herramienta y su manual de funcionamiento, se puede remitir a <https://latam.kaspersky.com/antivirus> | Hombre usando software de protección antivirus en el ordenador - Foto de stock de Acontecimiento libre de derechos |
| Firewall | Sistema para 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.  Para conocer la herramienta y su manual de funcionamiento, se puede remitir a <https://www.mcafee.com/support/?page=shell&shell=article-view&locale=es-ES&articleId=TS100887> | Empresa isométrica Internet security firewall protección información - arte vectorial de Servidor de seguridad libre de derechos |
| Proxy | Programa o dispositivo físico, que actúa de intermediario entre conexiones del navegador e internet, filtrando todos los paquetes entre ambos.  Para conocer la herramienta y su manual de funcionamiento, se puede remitir a <https://www.avast.com/es-es/c-topic-proxy> | Un par de operadores de servidor web de datos - arte vectorial de Base de datos libre de derechos |
| PKI - Public Key Infrastructure | Herramienta que permite el intercambio de datos en forma segura a través de Internet, y a su vez, verifica la identidad de la otra parte.  Para conocer la herramienta y su manual de funcionamiento, se puede remitir a <https://support.kaspersky.com/ksc/sp3/en-US/89287.htm> | El trabajo en equipo de los socios conecta piezas del rompecabezas como la integración y el inicio - Foto de stock de Fusiones y adquisiciones libre de derechos |
| MDR – Managed Detection and Response | Es un servicio en seguridad avanzado, donde se proporciona la búsqueda de amenazas, y monitoreo inteligente de las mismas.  Para conocer la herramienta y su manual de funcionamiento, se puede remitir a <https://www.mcafee.com/content/enterprise/fr-fr/security-awareness/endpoint/what-is-managed-detection-response.html> | Mensaje de pantalla de alerta de advertencia detectado por virus - arte vectorial de Amenazas libre de derechos |
| Pentesting | Son pruebas que realizan los expertos mediante técnicas avanzadas para detectar posibles amenazas o áreas con puntos débiles que los piratas informáticos pueden aprovechar.  Para conocer la herramienta y su manual de funcionamiento, se puede remitir a <https://pentest-tools.com/> | Pentesting Software Iconos Isométricos Conjunto Vector - arte vectorial de Grupo de iconos libre de derechos |

**2.4. Documentación de los 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 de los procesos | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración (voz en off)** | **Texto** |
| **1** | Con efectos para que las imágenes aparezcan en coherencia con el texto, puede ser como tipo carrusel.  Objetivo  bombilla de mano con tablero de destino para creativos y establecer el concepto de objetivo objetivo de negocio. - objetivos fotografías e imágenes de stock  **Cod.Imagen:** 233103\_CF6\_i032  Imagen de persona apuntando a un lugar específico  Seguridad  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de hombre con una espada enorme junto a un teléfono inteligente. escudo con cerradura. protección de datos en aplicaciones móviles, internet, mensajeros. ciberseguridad online. ilustración plana vectorial. - seguridad  Imágenes asociadas a seguridad, con candado  Privacidad  sistema de gestión de datos corporativos y sistema de gestión documental con privacidad de los empleados. confidencialidad de los empleados. software para la seguridad, búsqueda y gestión de archivos corporativos e información de empleados. - privacidad fotografías e imágenes de stock  **Cod.Imagen:** 233103\_CF6\_i034  Imágenes asociadas a la privacidad de la persona o empresa, datos privados o personales. | Un sonido o música de fondo | Uno de los objetivos del MSPI consiste en garantizar el eficiente manejo de los datos públicos, los cuales son representados como los activos digitales más valiosos que permiten la toma de decisiones. En este modelo se puede discriminar dos enfoques:  **De seguridad:** Se trata de generar incertidumbre detectando las falencias de ciberseguridad en la entidad.  **De privacidad:** Garantiza la protección de derechos a la intimidad y el buen nombre, así como la custodia de los secretos profesionales, industriales o de información privilegiada de terceros. | Objetivo principal del MSPI: garantizar el eficiente manejo de los datos públicos  Enfoque de seguridad  Enfoque de privacidad |
| **2** | Personas realizando trabajos con equipos de cómputo donde se visualice que ejecuta un antivirus, firewall…  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de protección de datos de privacidad, plantilla de página de aterrizaje de red privada virtual de internet. personajes diminutos alrededor de enorme portátil - seguridad digital  **Cod.Imagen:** 233103\_CF6\_i035  empresario mirando un registro de seguridad antivirus en pantalla en un equipo. - antivirus fotografías e imágenes de stock  **Cod.Imagen:** 233103\_CF6\_i036 | Un sonido o música de fondo | Los funcionarios que estén mejor capacitados con los procesos de seguridad y privacidad deben relacionar estos conocimientos con el tratamiento y uso de la información, así como acciones y medidas necesarias para la implementación de buenas prácticas cómo las siguientes:   * Sistema de información con la opción de recolección de datos personales. * Diseño e implementación de un sistema en gestión documental. * Políticas de PQR y atención al usuario. * Transferir información a terceros (entidades, países, etc.). | Funcionarios capacitados en buenas prácticas  Acciones y Medidas que garanticen la seguridad digital.   * Recolección de datos * Sistema en gestión documental. * Políticas de PQR y atención al usuario. * Transferir información a terceros (entidades, países, etc.). |
| **3** | Imagen en la que se visualicen cinco aspectos o etapas y un icono asociado a lal etapa, según las siguientes escenas  certificación de control de calidad, garantía comprobada de estándar. - sistema de gestion fotografías e imágenes de stock  **Cod.Imagen:** 233103\_CF6\_i037 | Un sonido o música de fondo | El MSPI es un instrumento con cinco etapas que protocoliza a las entidades en la implementación de las políticas de seguridad y privacidad de la información, en la forma y uso de documentos que faciliten el entendimiento entre todos los funcionarios de la entidad.  Cada una de las etapas, debe contar con un análisis que permita reflejar una matriz de riesgos que pondere la probabilidad de ocurrencia de los riesgos o incidentes (baja-intermedia-alta). | MSPI – instrumento que se ejecuta en cinco etapas |
| **4** | La misma imagen diseñada en la escena 3, pero que a medida que se narra cada etapa aparezca el nombre y el icono.    **Cod.Imagen:** 233103\_CF6\_i038 | Un sonido o música de fondo | A continuación, se presentan las etapas, los resultados esperados y los instrumentos usados en el MSPI.  En la etapa de diagnóstico se debe obtener como resultado un documento con los hallazgos del diagnóstico, con la identificación de activos de información que cuente con los datos personales.  El instrumento que se debe utilizar es la herramienta de diagnóstico. | Etapas de los instrumentos:   1. Diagnóstico 2. Planificación 3. Implementación 4. Evaluación 5. Mejora continua   Primera etapa: Diagnóstico  -Hallazgos o resultados |
| **5** | **Cod.Imagen:** 233103\_CF6\_i039 | Un sonido o música de fondo | Para la etapa de planificación, como resultado se deben contemplar los siguientes documentos:  -Las políticas de privacidad, aprobada por dirección y socializada con todos los funcionarios.  -Manual de políticas de SPI, aprobada por dirección y socializada con todos los funcionarios.  -Plan de gestión de privacidad de la información, aprobado por dirección.  Los instrumentos a utilizar son las herramientas de diagnóstico, roles, responsabilidades de Seguridad y privacidad de la Información. | Etapa de planificación  -Políticas de privacidad  -Manual de políticas del SPI  -Plan de gestión de privacidad de la información |
| **6** | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de icono de ubicación de la fallecimiento del coronavirus, concepto covid-19 - mapa de riesgos icono  **Cod.Imagen:** 233103\_CF6\_i040 | Un sonido o música de fondo | En la implementación, los resultados a entregar son:  -Documento de mapa de riesgos de privacidad de la información y acciones de solución de incidentes.  -Documento con el registro de las Bases de datos.  -Documento con la información clasificada, reservada, revisada y procedimientos ajustados.  Cómo instrumento único a usar está la herramienta de diagnóstico. Gestión de riesgos | Etapa de implementación:  -Mapa de riesgos de privacidad de la información  -Registro de las bases de datos  -Información clasificada |
| **7** | **Cod.Imagen:** 233103\_CF6\_i041 | Un sonido o música de fondo | En la etapa de evaluación de desempeño, son dos documentos que se deben entregar como resultados, el Plan de Seguimiento y el Plan de auditoría interna.  El instrumento a aplicar es la evaluación del desempeño, de la auditoria, del plan de comunicación, sensibilización y capacitación | Etapa de evaluación:  -Plan de Seguimiento  -Plan de auditoría interna. |
| **8** |  | Un sonido o música de fondo | En la etapa final referente a la mejora continua se debe garantizar la generación de documentos que describan:  -Los resultados del plan de seguimiento.  -Los resultados del plan de mejoramiento.  -El consolidado de las auditorias.  El instrumento que se debe aplicar es la evaluación del desempeño y mejora continua. (508) | Etapa de Mejora Continua  Los resultados del plan de seguimiento.  -Los resultados del plan de mejoramiento.  -El consolidado de las auditorias. |
| **Nombre del archivo** | **233103\_CF06\_v2.mp3** | | | |

**SINTESIS**

| **Tipo de recurso** | Síntesis |
| --- | --- |
| Control de la seguridad digital  Síntesis: Ciberseguridad y documentación de incidentes | |
| **Introducción** | En el siguiente diagrama encontrará un resumen de conceptos y palabras claves de los temas abordados en este contenido formativo. |
|  | |

**ACTIVIDAD DIDÁCTICA**

| **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 seguridad informática de la red de internet - ciberseguridad |
| Momentos política de Gobierno Digital | | Conocer, planear, ejecutar, medir |
| Fase de planificación | | Se utilizan como insumos los resultados de la etapa de diagnóstico para elaborar los informes con el método de SPI |
| ISO/IEC 27000 | | Procesos que permiten gestionar y dar tratamiento a los incidentes de la ciberseguridad |
| Ejecutar | | Tic para el estado y Tic para la sociedad |
| Contexto | | Se debe conocer, investigar y hallar oportunidades de mejora dentro del MSPI, para determinar los alcances del mismo |
| MSPI | | Diagnóstico, Planificación, Implementación, Evaluación de desempeño, Mejora continua |
| Fase de diagnóstico | | Se identifica la operatividad de la red de datos según procedimientos técnicos y marcos de referencia |
| Auditoría de código | | Realizar pruebas de código a las App que se usan en la entidad |
| Auditoría web | | El objetivo es detectar la seguridad del servidor y la página web de la entidad |
| Hacking ético | | Se realiza una serie de ciberataques para detectar la vulnerabilidad de la entidad. |

RESULTADOS:

**>= 7/10** – FELICITACIONES – Estimado aprendiz, ha comprendido la temática del componente formativo.

**< 7/10** – Estimado aprendiz, por favor revisar nuevamente el contenido del componente formativo e intente realizar nuevamente el test.

**MATERIAL COMPLEMENTARIO**

| Tipo de recurso | Material complementario | | |
| --- | --- | --- | --- |
| Tema | Referencia APA del material | tipo | Enlace |
| Glosario ISO 27000 | International Organization for Standardization. Glosario ISO 27000. 2009. Web. | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_virtualprovpro4391> |
| Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000 | Javier Valencia-Duque, Francisco, and Mauricio Orozco-Alzate. "Metodología Para La Implementación De Un Sistema De Gestión De Seguridad De La Información Basado En La Familia De Normas ISO/IEC 27000." RISTI : Revista Ibérica De Sistemas E Tecnologias De Informação 22 (2017): 73-88. Web. | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_scielo_journals_S1646_98952017000200006> |
| Seguridad en informática : seguridad, auditoría, cortafuegos, ingeniería social, ISO 27000 | Catellanos H, Luis R. Seguridad En Informática : Seguridad, Auditoría, Cortafuegos, Ingeniería Social, ISO 27000. Saarbrücken, Alemania: Editorial Académica Española, 2012. Print. | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000083567> |

**GLOSARIO**

| **Tipo de recurso** | Glosario |
| --- | --- |
| Auditoría | acciones que van enmarcadas a través de buenas prácticas normalizadas por ISO 27000, permite detectar, enlistar y documentar aquellas incidencias y vulnerabilidades en la infraestructura TIC de la entidad. |
| Control y planeación operacional | la entidad planifica, implementa y controla todos los procesos indispensables que permitan cumplir con todas las condiciones necesarias de SPI. |
| Diagnóstico | identifica la operatividad de la red de datos según procedimientos técnicos y marcos de referencia. |
| Gobierno en línea | permite centrarse en los componentes de Tecnología de la Información y Comunicaciones TIC para gestionar aportes que incluyen la formulación, gestión e implementación de un modelo de seguridad enfocado en salvaguardar la disponibilidad, integridad, transparencia y confidencialidad de los activos y datos digitales. |
| Indicadores de gestión | medición de eficiencia y efectividad en las acciones implementadas en SPI. Los indicadores permiten medir eficiencia, efectividad, y mejora continua. |
| Norma | describen lineamientos para el seguimiento de eventos, incidentes y acciones que lleguen a impactar en el desempeño de los sistemas de seguridad de la información en las empresas. |
| Plan de tratamiento de riesgos de SPI | Se identifican los controles que se deben aplicar en la gestión de los riesgos, para que éstos lleguen a un nivel aceptable. |
| Planeación | plantear acciones y objetivos, de tal manera que se cree la hoja de ruta para abordaje de eventos e incidentes. |
| Planificación | Etapa en la que se determinan los procesos que se deben implementar a nivel de SPI, mediante la estructura de gestión del riesgo en la operación de la red de datos. |
| Sistema de gestión sostenible | generan la percepción y aceptación de un estado más transparente, abierto al público, participativo y colaborativo, garantizando que la información entregada al ciudadano cuenta con controles y criterios de seguridad, documentado cada incidente que altere o modifique algún dato dentro del universo de información almacenada. |
| Soporte | medio de apoyo que documenta la entrega de recursos y competencias a cada área de manera oficial, mediante sensibilizaciones y comunicaciones. |

**REFERENTES BIBLIOGRÁFICOS**

| **Tipo de recurso** | Bibliografía |
| --- | --- |
| Asobancaria, 2020. Guía de buenas prácticas para auditar la ciberseguridad. Recuperado de: <https://www.asobancaria.com/wp-content/uploads/2020/09/Gui%CC%81a-de-Buenas-Pra%CC%81cticas-para-Auditar-la-CiberseguridadV4_compressed.pdf> | |
| CONPES, 2011. Lineamientos de política para la Ciberseguridad y Ciberdefensa. Recuperado de: <https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf> | |
| Decreto 1510 de 2013. Sistema de compras y contratación Pública. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53776> | |
| Decreto 2364 de 2012. Firma electrónica. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583> | |
| Decreto 2609 de 2012. Expediente electrónico. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50958> | |
| Decreto 2693 de 2012. Gobierno en línea. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51198> | |
| Decreto 333 de 2014. Entidades de certificación. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56767> | |
| Decreto Ley 019 de 2012. Racionalizar trámites a través de medios electrónicos. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=45322> | |
| EALDE Business School, 2021. Consejos para hacer una auditoría de seguridad informática para evitar riesgos digitales. Recuperado de: <https://www.ealde.es/auditoria-de-seguridad-informatica/> | |
| Kaspersky, 2022. Protección esencial contra virus para la PC. Recuperado de: <https://latam.kaspersky.com/antivirus> | |
| Ley 1150 de 2007. Seguridad de la información en contratación pública. Recuperado de: <http://www.oas.org/juridico/spanish/mesicic3_col_ley1150.pdf> | |
| Ley 1266 de 2008. Habeas data. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=HABEAS%20DATA&text=Dicta%20las%20disposiciones%20generales%20del,la%20proveniente%20de%20terceros%20pa%C3%ADses> | |
| Ley 1273 de 2009. Protección de información de los datos. Recuperado de: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> | |
| Ley 1341 de 2009. Principios y conceptos sobre la sociedad de la información y la organización de las TIC. Recuperado de: funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913 | |
| Decreto 1377 de 2013. Protección de datos. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646> | |
| Ley 1437 de 2011. Procedimiento Administrativo y de lo Contencioso Administrativo. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=41249> | |
| Ley 1480 de 2011. Estatuto del consumidor. Recuperado de: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Leyes/2011/Ley_1480_Estatuto_Consumidor.pdf> | |
| Ley 1581 de 2012. Protección de datos personales. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981> | |
| Ley 1712 de 2014. Transparencia y derecho al acceso a la información pública nacional. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882> | |
| LEY 1928 de 2018 [CONGRESO DE COLOMBIA]. Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest. Diario oficial 50664 DE JULIO 24 DE 2018, 24 de julio de 2018. COLECCIÓN DE LEGISLACIÓN COLOMBIANA. Legis Editores. <https://xperta.legis.co/visor/legcol/legcol_bf13eeed23da4ca4bbc9653685bd73ea020nf9/coleccion-de-legislacion-colombiana/ley-1928-de-julio-24-de-2018> | |
| Ley 527 de 1999. Validez jurídica y probatoria de la información electrónica. Recuperado de: <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> | |
| Ley 594 de 2000. Ley General de Archivos. Recuperado de: <https://normativa.archivogeneral.gov.co/ley-594-de-2000/> | |
| Ley 679 de 2001. Prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores. Recuperado de: <http://www.oas.org/juridico/spanish/cyb_col_ley_679_2001.pdf> | |
| Ley 962 de 2005.Simplificación y Racionalización de Trámites y procedimientos administrativos. Recuperado de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=17004#:~:text=%E2%80%9CPor%20la%20cual%20se%20dictan,p%C3%BAblicas%20o%20prestan%20servicios%20p%C3%BAblicos.%E2%80%9D> | |
| MANUAL DE GOBIERNO DIGITAL, 2018. Gobierno Digital. Recuperado de: Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) | |
| Mcafee, 2022. Cómo abrir un puerto en McAfee Firewall. Recuperado de: <https://www.mcafee.com/support/?page=shell&shell=article-view&locale=es-ES&articleId=TS100887> | |
| MDR, 2022. Virus detected warning alert message on computer screen, vector internet cyber security background. Hacking attack and virus detection spyware or digital antivirus malware for internet data fraud. Recuperado de: <https://www.mcafee.com/content/enterprise/fr-fr/security-awareness/endpoint/what-is-managed-detection-response.html> | |
| MinTic, 2016. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información. Recuperado de: Modelo de Seguridad y Privacidad de la Información | |
| Pentesting, 2022. Your pentesting arsenal, ready to go. Recuperado de: <https://pentest-tools.com/> | |
| PKI, 2022. Integration with public key infrastructure. Recuperado de: <https://support.kaspersky.com/ksc/sp3/en-US/89287.htm> | |
| Policía Nacional de Colombia, 2014. CIBERSEGURIDAD ENTORNO COLOMBIANO. Recuperado de: <https://www.oas.org/juridico/spanish/cyber/cyb8_col.pdf> | |
| Proxy, 2022. ¿Qué es un servidor proxy y cómo funciona? Recuperado de: <https://www.avast.com/es-es/c-topic-proxy> | |

**CONTROL DEL DOCUMENTO**

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

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

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