Guion para desarrollo de contenidos

| 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 | 220501111-04 - Validar el impacto de incidentes de seguridad con base en criterios técnicos y herramientas de monitoreo de acuerdo con el modelo del negocio. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 8 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Ciberseguridad - Impacto de eventos e incidentes |
| BREVE DESCRIPCIÓN | En este material se introduce al aprendiz en la validación del impacto de incidentes de seguridad con base en criterios técnicos y herramientas de monitoreo, de acuerdo con el modelo del negocio. Para ello, se hace necesario revisar, clasificar, validar y notificar el estado del incidente de acuerdo a una política de gestión de eventos e incidentes. |
| PALABRAS CLAVE | Centro de control de incidentes, centro de gestión de incidentes, CERT, CSIRT. |

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

# **TABLA DE CONTENIDOS**

**Introducción**

**1. Validación de Incidentes**

1.1 CSIRT

1.2 CERT

1.3 Centro de gestión de incidentes

1.4 Ciclo de gestión de incidentes

**2. Monitoreo de eventos**

2.1 Plataformas de seguridad

2.2 Notificación de respuestas

**INTRODUCCIÓN**

| Cuadro de texto |
| --- |
| Con un mundo cada vez más conectado a través de la Internet, los ataques, incidentes o eventos que afectan la seguridad de las instituciones son muy comunes, por lo que se ha hecho necesario verificar el impacto que pueden tener; para ello se requiere de una estructura y metodología organizacional que permita gestionar respuestas a través de ciclos de gestión.  En este componente formativo se describe la validación del impacto de incidentes de ciberseguridad enfocando el estudio en los Equipos de Respuesta ante Emergencias Informáticas (CERT), y los Equipos de Respuesta a Incidentes de Seguridad (CSIRT), además de realizar un acercamiento a los centros de gestión de respuesta a incidentes, las plataformas de monitoreo de eventos de seguridad y finalmente los ciclos de gestión (preparación, detección, análisis, notificación, documentación y gestión del conocimiento).  Para iniciar con el desarrollo temático se le invi ta a observar el siguiente video introductorio, en el que se detalla la temática a desarrollar y su importancia en los procesos empresariales asociados a la seguridad de la información. |

**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** | Eventos e incidentes | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración** | **Texto** |
| **1** | Recrear un oficial de vigilancia militar trabajando en una operación de seguimiento de la ciudad en un sitio de la oficina central para el control cibernético y el monitoreo para la gestión de la seguridad nacional, la tecnología y las comunicaciones del ejército.  oficial de vigilancia militar trabajando en una operación de seguimiento de la ciudad en un centro de la oficina central para el control cibernético y el monitoreo para la gestión de la seguridad nacional, la tecnología y las comunicaciones del ejérci - equipo seguridad digital fotografías e imágenes de stock | Por favor dejar música instrumental o ambiental | Según el CONPES 3701, donde se definen los lineamientos de política para la ciberseguridad y ciberdefensa, para el resguardo de la información almacenada en dispositivos tecnológicos se hace necesaria la creación de equipos especializados en incidentes de seguridad, los cuales proporcionan servicios para dar una respuesta oportuna a las entidades estatales; de este modo, aportan en el fortalecimiento de la ciberseguridad, generando confianza en los ciudadanos. | CONPES 3701  Lineamientos de política para la ciberseguridad y ciberdefensa.  Equipos especializados en incidentes de seguridad informática. |
| **2** | Un equipo de ingenieros profesionales de ciencias de datos informáticos que trabajan en escritorios con pantallas que muestran gráficos, infografías, datos técnicos de redes neuronales y estadísticas. Sala de control y monitoreo.Equipo de Ingenieros Profesionales de Ciencias de Datos Informáticos trabajan en escritorios con pantallas que muestran gráficos, gráficos, infografías, datos técnicos de redes neuronales y estadísticas. Sala de Control y Monitoreo Oscuro. | Por favor dejar música instrumental o ambiental | Todas las iniciativas que se puedan implementar, tanto en entidades públicas como privadas, permiten la mitigación de riesgos y la gestión de incidentes, generando roles y equipos encargados de la implementación de políticas de seguridad de la información (PSI). Para entender mejor la aplicación de esta, se hace necesario recordar el significado de evento y de incidente: | Generar iniciativas para:  Mitigación de riesgos  Gestión de incidentes |
| **3** | Recrear un ingeniero(a) con unos equipos de cómputo que evidencien acciones sospechosas como de *hacker o* que en las pantallas se evidencie mensajes de alertas.  sistema informático hackeado. pantalla de software de virus - ataques ciberneticos fotografías e imágenes de stock  Recrear un sistema interno tipo circuitos que muestre fallas o acciones de riesgo que atenten contra los datos como los virus.  microchip procesando datos a través del circuito de la placa base de la computadora - ataques ciberneticos fotografías e imágenes de stock | Por favor dejar música instrumental o ambiental | Evento: Es una situación que al presentarse denota una posible vulneración en las políticas de seguridad de la información (PSI) o fallas significativas en los protocolos de control. Los eventos pueden o no ocurrir, sin embargo, se pueden apreciar como incumplimientos en la implementación de las PSI o acciones sospechosas que pretenden sustraer datos de los sistemas o aplicaciones. | Eventos pueden ser:  -Vulneración de las políticas de seguridad  -Fallas significativas  -Acciones sospechosas |
| **4** | Recrear una serie de bloques con datos o simplemente un panel en el que se evidencia que tienen seguridad o protección pero ha sido violado uno de esos seguros.  cifrado de sus datos. cerradura digital. ataque de hackers y violación de datos. big data con código informático cifrado. proteja sus datos. concepto de seguridad y privacidad en internet cibernética. ilustración 3d de almacenamiento de base de datos - incidente seguridad informatica fotografías e imágenes de stock  Recrear una empresa en operación o un grupo de equipos que se evidencie que está siendo interrumpido su funcionamiento por un problema asociado a *hackeo,* que no permite el funcionamiento de los demás elementos.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de gestión de datos de prueba - tdm - supervisión del rendimiento de la aplicación - ilustración 3d - incidente seguridad informatica | Por favor dejar música instrumental o ambiental | Incidente: Suceso no deseado y no planeado que puede causar daño. Según la norma ISO 27035 ‘Gestión de incidentes de Seguridad Informática, SI’, el incidente se describe como un evento o una serie de eventos inesperados que tienen una alta probabilidad de comprometer o interrumpir la operatividad de la entidad o empresa, amenazando la seguridad informática y pudiendo afectar la transparencia, confidencialidad, disponibilidad e integridad de la información de la entidad o los equipos que la almacenan y gestionan. | **Incidente.** Serie de eventos de seguridad informática  -Comprometen o interrumpen la operatividad de la empresa |
| **4** | Un PC en el que se pueda evidenciar una alerta.  buscar advertencia hackeada en la computadora portátil concepto de datos de privacidad que son hackeados y violados de la amenaza de la tecnología de internet. renderizado 3d. - ataques ciberneticos fotografías e imágenes de stock  Reunión en la sala de conferencias de la oficina: el equipo de altos directivos dirige, hacen una lluvia de ideas, usan una computadora portátil. Los socios comerciales discuten informes financieros, planifican operaciones basadas en informes de líderes.  Reunión en la sala de conferencias de la oficina: el equipo diverso de altos directivos habla, hace una lluvia de ideas, usa una computadora portátil. Los socios comerciales discuten informes financieros, planifican operaciones basadas en informes de lí  primer plano enfoque en las manos de la persona escribiendo en el teclado de la computadora de escritorio. las pantallas muestran la interfaz de usuario del lenguaje de codificación. ingeniero de software crea innovadora aplicación de comercio electróni - ataques ciberneticos fotografías e imágenes de stock | Por favor dejar música instrumental o ambiental | Es de gran importancia diferenciar un evento de un incidente en SI, por lo que es importante hacer el análisis, estudio y documentación de estos para poder determinar su prioridad y así generar acciones a implementar en los casos que tengan similitud, minimizando el impacto que pueda tener en la organización.  Este proceso de documentación debe estar en continua actualización y ser publicado o socializado a todos los miembros de la empresa. | -Conocer las diferencias entre eventos e incidentes.  -Determinar prioridad.  -Generar acciones.  -Minimizar impacto.  -Documentar cada caso y socializarlo con los integrantes de la empresa. |
| **5** | Profesionales e ingenieros trabajando en el centro de control de sistema completo con monitores y servidores. También puede recrearse un supervisor con una *laptop* y llevar a cabo una reunión informativa. Posiblemente la agencia gubernamental realiza la investigación.  Profesional ingenieros trabajando en el centro de Control de sistema completo de monitores y servidores. Supervisor tiene Laptop y lleva a cabo una reunión informativa. Posiblemente la agencia gubernamental realiza investigación. | Por favor dejar música instrumental o ambiental | Como futuro técnico en el área de la seguridad digital, es su deber tener claros los conocimientos para revisar las políticas, clasificar los eventos e incidentes, validar su impacto y notificar al equipo de respuestas de la organización. Para la gestión de eventos e incidentes se debe tener en cuenta lo siguiente:   * CSIRTIS. * CERT. * Centros de gestión de respuesta a incidentes. * Plataformas de monitoreo de eventos de seguridad. * Ciclo de gestión de incidentes (preparación, detección y análisis, notificación, documentación y gestión del conocimiento). | Gestión de eventos e incidentes   * CSIRTIS. * CERT. * Centros de gestión de respuesta a incidentes. * Plataformas de monitoreo. * Ciclo de gestión de incidentes |
| **6** | Diferentes íconos asociados a seguridad como datos, registros, búsquedas y política o justicia, por ejemplo, la balanza.  reglas para el cumplimiento de los conceptos de tecnología empresarial de políticas - politicas de seguridad fotografías e imágenes de stock  Un PC en el que se evidencien varios elementos asociados a datos que se clasifican y organizan  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de el concepto de un sitio web de protección de datos, entrada prohibida. el concepto de seguridad online. la computadora portátil está protegida por una pantalla y un candado, ingresando una contraseña personal. ilustración vectorial isométrica - politicas de seguridad  Dos ingenieros de seguridad que estén revisando o validando información asociada a peligros de ataques cibernéticos.  sistemas de ciberseguridad para redes empresariales - equipo seguridad informatica fotografías e imágenes de stock | Por favor dejar música instrumental o ambiental | Por otro lado, para validar el impacto de los incidentes de seguridad se debe verificar la aplicabilidad de las políticas de seguridad de la información (PSI), revisar los elementos del incidente según criterios técnicos y parámetros, clasificarlo según políticas establecidas y notificar al equipo de respuestas de la organización según procedimientos establecidos. Así que sin más preámbulo, se le da la bienvenida al estudio de este componente formativo. (500) | Verificar la aplicabilidad de las políticas de seguridad de la información (PSI):  -Revisar los elementos  -Clasificar los eventos e incidentes  -Notificar al equipo |
| **Nombre del archivo** | **233103\_CF08\_v1.mp3** | | | |

**DESARROLLO DE CONTENIDO**

**1.** **Validación de incidentes**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| En el día a día se pueden cometer incidentes de seguridad inadvertidamente, por esto es necesario describir algunas situaciones, a manera de ejemplo, para no caer en estos errores, bien sea por desconocimiento, descuido o imprudencia.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de sistema hackeado, mensaje de alerta de advertencia en la pantalla - hacker  **Imagen:** 233103\_i01 | |

**Situación 1.**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Cuando se usa el correo corporativo para iniciar sesión o registrarse en alguna red social, o simplemente para publicar el nombre o logo de la empresa para la cual se trabaja, o fotografías donde quede expuesta la imagen corporativa; se debe evitar realizar bromas y comentarios que pueden llegar a afectar el perfil personal o profesional.  teléfono móvil sobre fondo azul con foto compartida en la aplicación de redes sociales - publicar fotos en redes sociales fotografías e imágenes de stock  **Imagen:** 233103\_i02 | |

**Situación 2**

| **Tipo de recurso** | Slider Presentación | |
| --- | --- | --- |
| **Introducción** | Exponer información en el puesto de trabajo, bien sea por descuido o dejando notas pegadas en el escritorio con información sensible, como datos de acceso a plataformas, bancos y claves. A continuación se describe el comportamiento de unos personajes, ¿Con cuál de ellos se identifica? | |
| * El despistado Su lema es: ‘déjeme que yo entiendo mi desorden’, algunas de las características de este personaje son: * Todo está en su escritorio, notas, datos de acceso, etc. A la vista de todo el mundo. * Tiene una foto de su hijo cuando era bebé, pero este ya es todo un profesional. * Los últimos recibos de servicios públicos cancelados. * Dos ediciones de la revista Dinero.   El nivel de riesgo de este personaje es ‘muy alto’. | | joven hombre de negocios en el escritorio cubierto con notas a pegajosas en blanco - despistado en oficina fotografías e imágenes de stock  **Imagen:** 233103\_i03 |
| * El subordinado. Se caracteriza por: * Ordenar la información en carpetas, pero no guardarlas. * Usar nombres para las carpetas como; ‘Info nueva’, ‘Info personal’, ‘Info confidencial’, ‘*Top secret’*. * Su puesto de trabajo está despejado pero guarda un paquete de documentos en un lugar visible con el nombre “confidencial”. * Cierra las gavetas del archivador con llave, pero guarda las llaves en el *mug* de los lapiceros.   Nivel de riesgo de este personaje es ‘medio’. | | Desesperada mujer asiática por estrés dolor de cabeza deprimido por la puesta en marcha de una pequeña empresa en la oficina en casa. Fracaso mujer de negocios trabajar en la oficina en casa. El empresario vendedor en línea tiene problemas de entrega d  **Imagen:** 233103\_i04 |
| * El segurísimo. Sus características son:   + Todo está protegido y bajo llave, hasta el teclado.   + Toda su información está clasificada como ‘confidencial’, hasta las notas escritas.   + Su escritorio es pulcro, no se ve ni siquiera el pequeño residuo de un tajalápiz.   + Tiene un *software* que le permite cambiar sus contraseñas constantemente.   + Los fines de semana va a la oficina a revisar su puesto de trabajo.   Nivel de riesgo de este personaje es ‘bajo’. | | Equipo de limpieza conserje en oficina  **Imagen:** 233103\_i05 |
| * El ejemplar. Sus características son: * Ordena, clasifica y nombra de forma adecuada su información. * Tiene presente lo que se puede guardar en el escritorio y lo que no. * Deja las gavetas de su archivador bajo llave, la cual lleva consigo siempre. * Nunca deja el PC desatendido y desbloqueado. Usa el comando *Windows + L* y su usuario tiene un *password* con seguridad fuerte. * Socializa y ayuda a implementar la cultura de Seguridad de la Información.   Nivel de riesgo de este personaje es ‘muy bajo’. | | mujer procesada seguridad de la información en línea - seguridad pc oficina fotografías e imágenes de stock  **Imagen:** 233103\_i06 |

**Situación 3**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Al reenviar correos masivos, como chistes o cadenas, y no usar la opción ‘CCO’ sino el espacio ‘para’, se está divulgando información sensible, como las cuentas de correo electrónico de terceros sin el consentimiento de los propietarios.  mensaje de conexión de comunicación a los contactos de correo electrónico teléfono concepto global de cartas - correos fotografías e imágenes de stock  **Imagen:** 233103\_i07 | |

**Situación 4**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Si se descargan programas, música, juegos, libros, etc., que cuentan con derechos de autor y se debe pagar por ellos, pero se accede a sus contenidos mediante plataformas que ofrecen estos servicios gratuitos, se está cometiendo un fraude al no respetar los derechos de autor y reproducir el contenido.  concepto de material protegido por derechos de autor con portátil - derechos de autor fotografías e imágenes de stock  **Imagen:** 233103\_i08  Existen muchas situaciones del diario vivir en las que se pueden estar cometiendo infracciones de manera involuntaria, poniendo en riesgo la seguridad digital. Es importante reflexionar y autoevaluarse para saber qué tipo de personaje se es y qué situación se está realizando, con el fin de corregir estos hábitos lo más pronto posible, evitando así cualquier inconveniente a futuro.  candado con el símbolo de copyright - derechos de autor fotografías e imágenes de stock  **Imagen:** 233103\_i09 | |

| Cuadro de texto |
| --- |
| Para validar los incidentes es necesario contar con equipos capacitados en seguridad digital, como los siguientes: |

* 1. **CSIRT**

| **Tipo de recurso** | | Pestañas o tabs verticales |
| --- | --- | --- |
| **Introducción** | | Con la masificación de las TIC, también aumentaron los ataques e incidentes de Seguridad de la Información como, por ejemplo, manipulación de redes de datos, alteración de cajeros electrónicos y transferencias bancarias, generando así pérdidas por billones de pesos. Por tal motivo, el Congreso de la República ha promulgado la Ley 1273 de 2009. Desde entonces, y como buenas prácticas para prevenir y minimizar la exposición a los ataques nacen los CSIRT. |
| concepto de negocio y tecnología. oficina inteligente. gui (graphical user interface). grupo de empresarios en la oficina. - equipo seguridad de la informacion fotografías e imágenes de stock  **Imagen:** 233103\_i10 | | |
| **Definición** | Los CSIRT son un equipo que tiene la función de prestar los servicios que permiten prevenir y dar respuesta a incidentes de seguridad de la información; se encargan generalmente de cubrir un área específica en una entidad pública o privada. | |
| **Objetivos** | Los CSIRTS pueden ser internos o externos cubriendo áreas para el manejo de incidentes en los centros de coordinación y análisis, los equipos de vendedores y proveedores. Estas acciones le permiten ser el punto central para el informe de problemas, cuyos objetivos se basan en:   * Verificar si se ha producido el incidente. * Recuperar la continuidad operativa de la empresa. * Disminuir las consecuencias del incidente. * Especificar la forma en que el ataque se convirtió en incidente. * Preparar la entidad para futuros incidentes. * Aumentar la seguridad digital y la respuesta a incidentes. * Dar seguimiento a las actividades ilegales. * Mantener informada de la gestión y respuesta a todos los miembros involucrados e interesados. | |
| **Servicios de un CSIRT** | * Servicios reactivos: son los que se inician cuando el incidente ya ocurrió, es decir, un equipo de oficina comprometido o infectado, intrusos en registros de información, *malware* disperso por toda la red, *software* vulnerado o eventos identificados sin mecanismos previos de protección. * Servicios proactivos: son aquellos que se presentan antes de ocurrir un suceso. Son los llamados servicios preventivos, los cuales se anticipan a los eventos e incidentes protegiendo y asegurando los activos de la información. * Servicios en gestión de calidad de SI: dan valor agregado a los reactivos y proactivos, además de ser complementarios a las buenas prácticas existentes en otros sectores como las Tecnologías de la Información (IT), auditorías o áreas de capacitación. | |
| **Funciones** | Las funciones del CSIRT se basan en el cumplimiento de los objetivos y la eficiencia del manejo de incidentes, entre las que se pueden destacar:   * Entregar información confiable de fuentes primarias. * Enviar alertas al CSIRT que corresponda. * Almacenar y seleccionar la información que se usará en los niveles posteriores. * Realizar los procesos de prevención y recuperación de incidentes recientes. | |
| **En conclusión** | El CSIRT es el encargado de coordinar las actividades de respuesta a los implicados de un incidente, por lo general, deben incluir a la víctima del incidente, terceros que se encuentren involucrados, y cualquier otra parte que necesite asistencia cuando se realice el análisis, por ejemplo, administradores de redes, soporte IT, proveedores de servicios de internet, otros CSIRT, etc. | |

| Cuadro de texto |
| --- |
| Es momento de continuar con los equipos que apoyan el proceso de validación de incidentes, los CERT. |

**1.2. CERT**

| **Tipo**  **de recurso** | Pestañas o tabs horizontales | |
| --- | --- | --- |
| **Introducción** | Los activos de información en una entidad deben ser preservados, y para ello se requiere de protección, ya sea con buenas prácticas de administración o mediante equipos que impidan el acceso no autorizado de usuarios a los repositorios de estos activos. | |
| **Definición** | El CERT (*Computer Emergency Response Team*) es el equipo para dar respuestas a las emergencias informáticas. Esta palabra es una marca registrada desde el año 1997 por parte de la *Carnegie Mellon University.* Aunque muchas empresas usan el término de forma genérica, es indispensable saber qué se debe solicitar permiso para su uso en la institución, so pena de estar infringiendo una norma legal. | el líder del equipo está hablando a través de un walkie-talkie en el sitio de construcción - equipo de emergencias informaticas fotografías e imágenes de stock  **Imagen:** 233103\_i11 |
| **Enfoque** | Según *Carnegie Mellon University* (2022), el CERT tiene un enfoque particular y un nicho que opera como un socio con el gobierno, la industria, el cumplimiento de la ley y el mundo académico para mejorar la seguridad y la capacidad de recuperación de los sistemas y redes informáticos. Este estudia problemas que tienen implicaciones generalizadas de ciberseguridad y desarrolla métodos y herramientas avanzados. | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de ciberseguridad, contraseñas seguras y registro del sitio. - seguridad digital  **Imagen:** 233103\_i12 |
| **Los CERT y la ciberseguridad** | La ciberseguridad a través del CERT está basada en la recepción, análisis y respuesta de novedades y acciones de incidentes de SI para las instituciones públicas y privadas, las cuales destinan sus recursos a la gestión de incidentes de SI y protección de infraestructuras críticas. | programadora de ti inteligente femenina que trabaja en computadora de escritorio en la sala de control del sistema del centro de datos. equipo de jóvenes profesionales que realizan programación de códigos - seguridad digital fotografías e imágenes de stock  **Imagen:** 233103\_i13 |
| **ColCERT** | En Colombia, el Ministerio de Defensa estructuró el ColCERT, que es el equipo coordinador a nivel nacional en aspectos de seguridad informática, el cual será el encargado de apoyar y colaborar con las demás instituciones a nivel nacional, como por ejemplo, el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético - CCOC. (Consejo Nacional de Política Económica y Social (CONPES), República de Colombia, y Departamento de Planeación (DNP), 2011). | **Figura 1**  *Modelo de Coordinación*    Fuente: Tomado del Consejo Nacional de Política Económica y Social –CONPES-, República de Colombia, y Departamento de Planeación –DNP-(2011) Lineamientos de Política para Ciberseguridad y Ciberdefensa. Conpes 3701. p. 21. <https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf>  **Imagen:** 233103\_i14 |
| **Misión del ColCERT** | El ColCERT es un grupo adscrito al Ministerio de Defensa Nacional, integrado por funcionarios civiles, personal militar y comisiones de otras entidades que debe cumplir con las directrices de la comisión intersectorial de diversas entidades; su misión es coordinar las acciones que se requieran para proteger la infraestructura TI del Estado colombiano, frente a incidencias y ataques que se puedan presentar y comprometan la seguridad nacional.  El ColCERT inició operaciones en el segundo semestre del año 2011, siguiendo un modelo relacional diseñado por el Ministerio de Defensa. (Consejo Nacional de Política Económica y Social (CONPES), República de Colombia y Departamento de PlaneaSción (DNP), 2011). | **Figura 2**  *Modelo Relacional del ColCERT.*    Fuente: Tomado del Consejo Nacional de Política Económica y Social –CONPES-, República de Colombia, y Departamento de Planeación –DNP-(2011) Lineamientos de Política para Ciberseguridad y Ciberdefensa. Conpes 3701. p. 24. <https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf>  **Imagen:** 233103\_i15 |

| Cuadro de texto |
| --- |
| El monitoreo continuo de los equipos que hacen parte de la red de seguridad de la información sigue unos protocolos o procedimientos descritos en la normatividad ISO 27000; estos deben ser establecidos o personalizados de acuerdo al tipo y necesidad de la empresa, a través del centro de gestión de incidentes, el cual se describe a continuación: |

**1.3. Centro de gestión de incidentes**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| El monitoreo trae consigo la operación de herramientas que protegen y controlan los activos, así como las herramientas de monitoreo y gestión de los incidentes que se puedan presentar.  agentes de policía en el centro de control de vigilancia - gestion de incidentes seguridad digital fotografías e imágenes de stock  **Imagen:** 233103\_i16 | |

| **Tipo de recurso** | Acordeón tipo 2 |
| --- | --- |
| **Introducción** | Un centro de gestión de incidentes cumple con varias etapas que conforman un proceso de atención de incidentes en SI, estas se encuentran organizadas de la siguiente manera: |
| **Figura 3**  *Flujograma de gestión de incidentes de SI*    Fuente: Instituto para la Economía Social -IPES (2017) Gestión de incidentes de seguridad de la información. p. 7. <https://www.ipes.gov.co/images/informes/SDE/Mapa_de_Procesos/Proceso_Gestion_de_seguridad_de_la_Informacion_y_Recursos_Tecnologicos/2020/In_069_Gestion_De_Incidentes_De_Seguridad.pdf.pdf>  **Imagen:** 233103\_i17 | |
| Preparación  Se intenta minimizar la cantidad de incidentes mediante la aplicación de controles basados en resultados de evaluación de riesgos. Es importante tener presente que hay una cierta cantidad de incidentes que no pueden ser tratados, estos se denominan residuales. | |
| Detección y análisis  Es fundamental mitigar el impacto de los incidentes por medio de acciones eficientes, logrando alertar a la entidad cada vez que exista una situación. Después que el incidente se haya gestionado, se debe realizar un informe detallando causas, costos y el paso a paso que se debe seguir cuando se presente en el futuro. | |
| Contención, erradicación y recuperación  Después de analizar y priorizar el incidente se procede a contener sus consecuencias y propagación. Las acciones por implementar deben ser previamente analizadas en conjunto con el equipo de atención. Cada situación se debe tratar como única, debido a sus formas y comportamientos particulares. Por lo general, algunas acciones que se implementan son:   * + Desconexión del sistema y redes cableadas o inalámbricas.   + Deshabilitar funciones del sistema y dejar el servicio en *off*.   + Revisión posterior del incidente. | |
| Recolección y manejo de evidencias  La recolección de evidencia y su posterior manejo debe realizarse con personal altamente entrenado y capacitado para llevar a cabo dichas acciones. Las evidencias son fundamentales para iniciar procesos judiciales contra los atacantes, pero deben ser recolectadas cumpliendo estándares y recomendaciones legales, de acuerdo al procedimiento estipulado por la entidad. | |

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| En Colombia existe el Comando de Atención Inmediata Virtual - CAI Virtual, un grupo coordinado por el ColCERT que previene, gestiona e investiga los incidentes que se presentan en SI; este recibe los reportes y la información de delitos cibernéticos, por lo tanto, debe clasificar y perfilar las conductas encontradas. Con ello busca la protección y respuesta de la ciudadanía ante delitos cibernéticos mediante acciones para prevenir, atender, investigar y apoyar en la judicialización de estos en el territorio nacional.  concepto de seguridad de red. protección cibernética. software antivirus. - equipo de seguridad digital fotografías e imágenes de stock  **Imagen:** 233103\_i18 | |

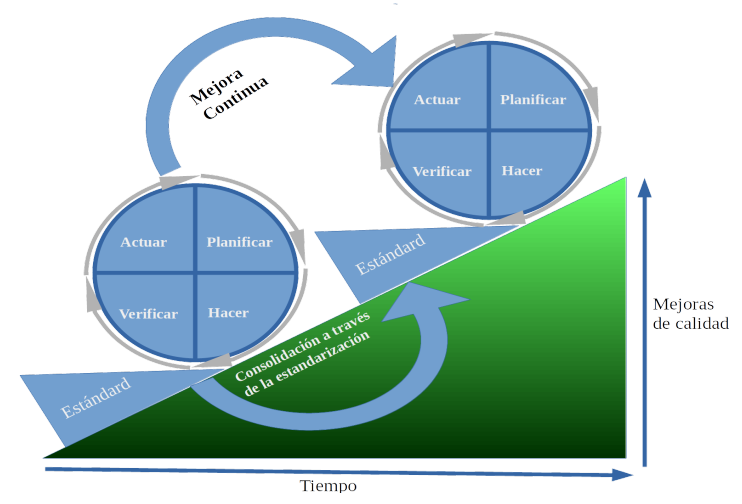
| Cuadro de texto |
| --- |
| Para finalizar con el primer tema de estudio sobre la validación de incidentes, es necesario reconocer las etapas del ciclo de gestión de incidentes, las cuales son las siguientes: |

**1.4. Ciclo de gestión de incidentes**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Con la implementación del CSIRT se deben considerar e implementar algunos factores que se rigen por los principios del ciclo de vida PHVA -Planificar-Hacer-Verificar-Actuar-, garantizando la mejora continua. | |

**Figura 4**

*Ilustración del ciclo de Deming (Ciclo PHVA)*



*Mejoras continuas a la calidad se logran iterando en el ciclo y consolidando el progreso logrado a través de la estandarización (Johannes Vietze).*

Fuente: Heide der van, M. (2020) *Estableciendo un CSIRT*. <https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf>

**Imagen:** 233103\_i19

| Cuadro de texto |
| --- |
| El equipo encargado del ciclo de la gestión de incidentes debe integrar como mínimo a un directivo de la organización, de tal manera que la aplicabilidad de las acciones no se desvíe del objeto misional de la entidad, y a su vez, que pueda suplir de forma rápida las necesidades que llegue a tener. |

| **Tipo de recurso** | Infografía estática |
| --- | --- |
| **Texto introductorio** | A continuación, se describen cada una de las etapas del ciclo de gestión de incidentes. |
| *Ciclo de gestión de incidentes*    <https://media.istockphoto.com/vectors/circle-diagram-infographic-with-flat-style-vector-id1320094390?k=20&m=1320094390&s=612x612&w=0&h=OyV7ysti3yK1zfV5II9OeGIXQy4-rkil_Z8kYWNCQzk=>  Texto para diseñador web   | **PLANIFICAR** | **HACER** | | --- | --- | | En esta etapa se define el marco para el CSIRT, además del presupuesto con todos los costos operacionales, para llevar a cabo las acciones de tratamiento de los incidentes. Este debe ser presentado ante la junta directiva de la organización. | Se implementa el plan de acción previamente planificado, que contiene las políticas para el manejo de incidentes e intercambio de información. | | **VERIFICAR** | **ACTUAR** | | Se realiza el análisis de desempeño grupal, teniendo en cuenta el cumplimiento de las tareas más importantes, involucrando a todos los miembros del equipo. | Se decide qué mejoras realizar al proceso, o qué acciones adicionales implementar, abarcando otras áreas o tipos de incidentes nuevos que se presenten. Iniciar nuevamente el ciclo con la etapa de ‘planificar’, con el propósito de implementar estas mejoras. |   Nota: Elaboración propia del experto con la información tomada de Heide der Van, M. (2020) *Estableciendo un CSIRT*. <https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf> | |
| **Código de la imagen** | 233103\_i020 |

| Cuadro de texto |
| --- |
| A continuación, se presenta a manera de ejemplo el ciclo completo de la gestión de incidentes de la organización española CEDIA: |

**Tabla 1.**

*Ejemplo del ciclo completo de la gestión de incidentes de la organización española CEDIA*

| **Nivel de Madurez** | **Descripción** |
| --- | --- |
| Introductorio | El CSIRT existe como un Punto de Contacto (POC) para coordinación y resolución de incidentes. Tiene sus reglas y regulaciones para notificar a las autoridades relevantes. |
| Básico | Igual a 1, añadiendo un proceso para manejar nuevas amenazas. Se utiliza un sistema de *tickets* para manejar los incidentes reportados y se proveen avisos para la organización. |
| Activo | Igual a 2, añadiendo herramientas de análisis de amenazas y procedimientos para la clasificación y el manejo de incidentes. |
| Proactivo | Igual a 3, adicionando la diseminación de información de seguridad, herramientas para verificar y mantener su estado y planificación de entrenamiento a miembros del equipo. |
| Comprensivo | Igual a 4, pero con monitoreo en tiempo real de incidentes y amenazas. Se definen y comparten por interno, se proporcionan terceras instrucciones para nuevas amenazas y formas de prevenir incidentes con la finalidad de generar conciencia. |

Fuente: Elaboración propia del experto con la información tomada Heide der Van, M. (2020) *Estableciendo un CSIRT*. <https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf>

| Cuadro de texto |
| --- |
| Ya se conocen los incidentes en la seguridad digital, es hora de ver qué son los eventos y cómo se deben monitorear. |

**2. Monitoreo de eventos**

| **Tipo de recurso** | Slider Hitos/ Línea de tiempo horizontal | |
| --- | --- | --- |
| **Introducción** | Es fundamental en la gestión de seguridad digital de las organizaciones que se rastreen los incidentes de seguridad digital, a continuación se describe cómo hacerlo: | |
| **¿Para qué monitorear los eventos?** | Con el aumento frenético y la sofisticación de las amenazas de ciberseguridad, se deben tomar acciones que recopilen y rastreen los incidentes en tiempo real, implementando análisis avanzados que ayuden a clasificar y enviar a un equipo de expertos la información necesaria para su posterior estudio. Los miembros deben seleccionar los datos y dar prioridad a los eventos, identificando los incidentes en los que necesitan enfocarse y aplicar acciones inmediatas. | diseño de páginas web. desarrollo de tecnologías de programación y codificación. - monitorear incidentes de seguridad digital fotografías e imágenes de stock  **Imagen:** 233103\_i21 |
| **¿Cómo monitorear?** | El monitoreo de eventos debe centrarse en las mejores prácticas de supervisión, implementando la automatización integrada con la revisión de los miembros del equipo de trabajo, esto permite descartar la mayor cantidad de eventos generados por falsas alarmas, para poder identificar las amenazas considerables y centrar los esfuerzos de validación y tratamiento en los problemas críticos. | 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. - monitorear incidentes de seguridad digital fotografías e imágenes de stock  **Imagen:** 233103\_i22 |
| **Monitoreo Continuo** | El monitoreo continuo se debe realizar a todos los elementos de la infraestructura que intervienen en el proceso de resguardo de la información, así como a los que se van integrando por motivo de crecimiento o automatización de gestión de los registros. De este modo, se podrán controlar todos los dispositivos y garantizar protección total a los sistemas de información, tomando mejores decisiones y manteniendo el cumplimiento normativo. | cerrar el programador man mano (empleado) escribir el lenguaje de la computadora (código binario) para introducir en el sistema de seguridad para proteger y prevenir el malware (virus) para el concepto de seguridad cibernética - monitorear incidentes de seguridad digital fotografías e imágenes de stock  **Imagen:** 233103\_i23  <https://media.istockphoto.com/photos/close-up-programmer-man-hand-typing-computer-language-to-input-on-picture-id1189523517?k=20&m=1189523517&s=612x612&w=0&h=KIl2KX7_2255awxCX7Cg7bzsP6xbk0GxUGgqlSazNwI=> |

| **Tipo de recurso** | Infografía interactiva Punto caliente | |
| --- | --- | --- |
| **Texto introductorio** | Un sistema de monitoreo confiable debe cumplir, como mínimo, las siguientes características: | |
| Características de un sistema de monitoreo    **Nota:** elaboración propia del experto. | | |
| **Código de la imagen** | 233103\_i24 | |
| **Punto caliente 1** | Relación entre dispositivos: proporcionar una correlación entre los dispositivos de la red y el equipo de reportes para que todos cuenten con la misma información al detalle y se pueda examinar minuciosamente. | Puede ir sobre cada título o icono |
| **Punto caliente 2** | Traducción de datos: traducir datos de difícil entendimiento en tiempo real, documentando la lista de acciones a realizar por la organización. | Puede ir sobre cada título o icono |
| **Punto caliente 3** | Priorización de actividades: ayudar a los equipos CSIRT y CERT en la priorización de actividades que previenen las alertas de falsos positivos, para ser más efectivos en la implementación de acciones en los eventos que realmente sean críticos. | Puede ir sobre cada título o icono |
| **Punto caliente 4** | Localización de amenazas: localizar las fuentes de las posibles amenazas y seguir el patrón de ataque, con el propósito de reforzar los puntos débiles e ir evolucionando hacia el desarrollo de la gestión de las amenazas más críticas. | Puede ir sobre cada título o icono |
| **Punto caliente 5** | Apoyarse en los CSIRT y el CERT: permitir que el CSIRT y el CERT realicen hipótesis ajustadas sobre los incidentes pasados que suministren el proceso para la prevención de eventos futuros. | Puede ir sobre cada título o icono |
| **Punto caliente 6** | Cumplimiento de la normatividad: garantizar la solución integral y que permita evolucionar la plataforma de seguridad de la entidad, sin necesidad de cambiarla para futuros eventos. | Puede ir sobre cada título o icono |

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| El monitoreo de la seguridad se identifica como una herramienta de prevención de SI, y a su vez, forma parte de su gestión. Para ello, los sistemas clasifican como indiferentes las alarmas que generan la detección de un incidente, sea este autorizado o no. Sin embargo, la creación del equipo CSIRT o CERT hace que este proceso sea más eficiente, detectando cambios o comportamientos poco usuales en las actividades, generando ‘alertas’ ante sospechas y recopilando la información necesaria para ser analizada, tomando acciones preventivas.  cámara de vigilancia en la ciudad y los iconos - monitoreo de seguridad fotografías e imágenes de stock  **Imagen:** 233103\_i25  Para reconocer algunas de las acciones que se realizan en el monitoreo de eventos, se le invita a ver el siguiente video. | |

| **Tipo de recurso** | Video animación 2D | | | |
| --- | --- | --- | --- | --- |
| **NOTA** | **La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente** | | | |
| **Título** | Ejemplo del monitoreo de eventos | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración** | **Texto** |
| **1** | Recrear un personaje que narre, puede ser similar a la siguiente figura.    Un equipo que esté monitoreando o vigilando a través de computadores y herramientas de audio  en la sala de supervisión apoyo técnico especialista habla en auricular. sus colegas están trabajando en segundo plano. - monitoreo de eventos de seguridad fotografías e imágenes de stock  Definir  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de detalle definido - definir icono  Cuantificar- medir      Controlar - supervisar | Música ambiental o instrumental de fondo y que tenga coherencia con las animaciones de texto e imágenes. | El monitoreo de eventos puede resultar ineficiente e infructuoso si no se mejora al pasar el tiempo, por lo tanto, se debe definir, cuantificar y medir la cantidad de incidentes, así como el impacto generado.  El monitoreo eficiente debe precisar lo siguiente:   * Tener control en las acciones de acuerdo a los niveles de servicio; debe contener como mínimo la fecha y hora de su intermitencia. * Supervisar los inventarios digitales y de la información. * Gestionar cualquier incidente y copias de seguridad para proteger a la organización de cualquier ataque de *ransomware.* * Verificar el funcionamiento y actualización de los antivirus. | Monitoreo de eventos requiere:  -Definir  -Cuantificar  -Medir cantidad de incidentes  Acciones:  -Control de acciones  -Supervisar inventarios digitales  -Gestionar incidentes  -Verificar funcionamiento de antivirus |
| **2** | El mismo personaje de la escena 1 narrando. Mostrar la fórmula  Recrear una imagen de un banco con el nombre: Banco digital 50K  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de banco - trabajando en un banco vector  Personas realizando diferentes actividades asociadas al sector financiero y al lado se puede ubicar la fórmula que está en el texto  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de grupo empresarial isométrico que trabaja en la flecha ascendente - trabajando en un banco vector | Música ambiental o instrumental de fondo y que tenga coherencia con las animaciones de texto e imágenes. | Como un ejemplo del monitoreo de eventos, se describe el siguiente caso hipotético:  La empresa ‘Banco digital 50K’ requiere monitorear y ejecutar los respaldos de información de manera semanal para ello, es primordial conocer el porcentaje de éxito que se tiene. El equipo CSIRT selecciona las métricas, el indicador a calcular estaría dado por la fracción: número de veces que se realiza correctamente, dividido entre el número de respaldos que se realizaron teniendo como límite de tiempo una semana. Este valor entregará un margen exacto del monitoreo realizado. | Ejemplo:  Empresa ‘Banco digital 50K’  Requiere conocer el  % éxito  Se calcula así:  El resultado es el margen de monitoreo realizado |
| **3** | El mismo personaje de la escena 1 narrando a la vez que el texto e imágenes se muestran, puede ser un PC o un tablero de oficina  Persona que destaque la prevención en la protección de datos con íconos de candados  botón de prevención de fraude, concepto sobre ciberseguridad y protección de tarjetas de crédito - prevenir ataques ciberneticos fotografías e imágenes de stock  Tarjeta de crédito, un dispositivo como PC y celular en los que se evidencie que se puede hacer pago electrónico.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de pago en línea, pago electrónico de facturas. aplicación de banca móvil y pago con tarjeta de crédito. - pago electrónico | Música ambiental o instrumental de fondo y que tenga coherencia con las animaciones de texto e imágenes. | En esta situación la prevención es el pilar fundamental. Por ejemplo, si el ‘Banco digital 50K’ implementa la plataforma de pago electrónico, debe regirse por un estándar de seguridad de los datos que está enmarcado por la industria de las tarjetas de crédito. El PCI DSS establece las medidas de envío de información que deben estar correctamente cifradas, y el uso del *firewall* que impide el acceso de intrusos a las bases de datos de los clientes. | La base es la ‘prevención’, así:  -Sí la empresa cuenta con pago electrónico 🡪Cumplir con estándar de seguridad |
| **4** | El mismo personaje de la escena 1 narrando a la vez qué textos e imágenes se muestran, puede ser un PC o un tablero de oficina  Imagen asociada a auditoría en seguridad  gerente de cuello blanco masculino tocando auditoría de seguridad - auditorias sistema de seguridad digital fotografías e imágenes de stock  Correcto funcionamiento de diferentes dispositivos y que además tenga un ícono o imagen de seguridad, como el candado  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de seguridad de datos de red y ciberdefensa - auditorias sistema de seguridad digital | Música ambiental o instrumental de fondo y que tenga coherencia con las animaciones de texto e imágenes. | Al implementar el sistema de gestión de seguridad de la información y sus auditorías, se asegura que los recursos funcionen y se usen de manera correcta. A su vez, el monitoreo logra generar informes de los certificados de seguridad que mantienen vigentes y actualizados los cifrados de la información, además de vigilar los *firewalls* de la entidad. | El sistema de gestión de seguridad de la información y sus auditorías  **->**  Garantizan el buen funcionamiento de los recursos |
| **5** | El mismo personaje de la escena 1 narrando a la vez qué textos e imágenes se muestran, puede ser un PC o un tablero de oficina  Mostrar la lista y al lado imágenes asociadas a la seguridad de los datos, antivirus, candados, *firewall*, claves, bloqueos, entre otros.  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de banner isométrico para protección de datos de internet - antivirus  seguridad cibernética. usando tecnología y el icono conexión de red de cliente de la tableta e intercambiar datos en la pantalla virtual. concepto de ataque cibernético - sistema de seguridad digital fotografías e imágenes de stock  ilustraciones, imágenes clip art, dibujos animados e iconos de stock de concepto de protección de datos. escaneo de huellas dactilares, sistema de identificación. estilo moderno de dibujos animados planos. ilustración vectorial - sistema de seguridad digital | Música ambiental o instrumental de fondo y que tenga coherencia con las animaciones de texto e imágenes. | De esta forma, el sistema de gestión de seguridad de la información aborda varios aspectos, que pueden incluir o no el monitoreo de eventos, entre estos se pueden destacar:   * Actualización y automatización de parches de seguridad. * Estado de la red, el antivirus y el *firewall.* * Capacitación del personal en prevención de fraudes (ingeniería social). * Usos de red, dispositivos móviles y recursos informáticos. * Fugas en los datos. * Cumplimiento con la ley 1581 de 2012. * Autoevaluación para implementar la gestión unificada de amenazas. * Auditoría de la red. * Análisis de correlación de los datos e incidentes. * Verificación del *firmware* instalado. * Pruebas de penetración y auditorías *web.* * Auditoría forense. | ¿Qué abarca el sistema de gestión de seguridad de la información?  Info para el Diseñador web: En este caso si considero necesario mostrar en texto la lista de aspectos, puede ser a manera de carrusel o como lista.  -Actualización y automatización de parches de seguridad.  -Estado de la red, el antivirus y el *firewall.*  -Capacitación del personal en prevención de fraudes (ingeniería social).  -Usos de red, dispositivos móviles, y recursos informáticos.  -Fugas en los datos.  -Cumplimiento con la ley 1581 de 2012.  -Autoevaluación para implementar la gestión unificada de amenazas.  -Auditoría de la red,  -Análisis de correlación de los datos e incidentes.  -Verificación del firmware instalado.  -Pruebas de penetración y auditorías *web.*  -Auditoría forense. |
| **6** | El mismo personaje de la escena 1 narrando a la vez qué textos e imágenes se muestran, puede ser un PC o un tablero de oficina  Computadores en los que se pueda visualizar en la pantalla una plataforma de seguridad que genere alertas  concepto de seguridad informática - antivirus fotografías e imágenes de stock  alerta de virus en una pantalla de ordenador portátil. ilustración 3d - antivirus fotografías e imágenes de stock | Música ambiental o instrumental de fondo y que tenga coherencia con las animaciones de texto e imágenes. | Sin embargo, toda gestión de incidentes debe contar con plataformas que garanticen la seguridad y que los sistemas no sufran elevadas consecuencias tras la detección de incidentes; es importante contar con herramientas de protección, y además, que los encargados cuenten con las habilidades y conocimientos para su funcionamiento.  En el siguiente tema se explican a detalle las plataformas en los sistemas de seguridad. (504) | La gestión de incidentes es más confiable si se realiza a través de plataformas. |
| **Nombre del archivo** | **233103\_CF08\_v2.mp3** | | | |

**2.1 Plataformas de seguridad**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Muchas compañías reconocidas a nivel global han centrado su objetivo comercial en crear plataformas y herramientas de ciberseguridad. Un caso particular que se puede considerar es la compañía DELL, que integra en su portafolio de productos y servicios las siguientes plataformas y herramientas: | |

| **Tipo de recurso** | Tarjetas Avatar | |
| --- | --- | --- |
| **Introducción** | A continuación, encontrará algunas de las soluciones de seguridad destacadas para las principales amenazas actuales, tomadas desde la página de la empresa DELL. | |
| Servicios de resistencia del negocio  Permite alinear las necesidades del negocio con las tecnologías, los procesos y el personal de TI para crear un programa de resiliencia del negocio integral. (DELL, 2022). | | **Imagen:** 233103\_i26  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| *Ransomware Defender* para DELL EMC *PowerScale*    Es una solución de protección cibernética integral para detectar patrones de acceso a datos inusuales, aislar los datos con espacio de aire y recuperar los datos de archivos y objetos. (DELL, 2022). | | **Imagen:** 233103\_i27  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| DELL *SafeData*  Conjunto de aplicaciones integradas en la solución *Dell Trusted Devices* que proporciona cifrado a nivel de disco y archivo, infraestructura de escalamiento de red SASE y persistencia de datos a prueba de manipulaciones en entornos de múltiples nubes. (DELL, 2022). | | **Imagen:** 233103\_i28  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| Servicios de seguridad de terminales de DELL  Serie de servicios integrales que ayuda a identificar riesgos, implementar soluciones y prevenir amenazas futuras con confianza. (DELL, 2022). | | **Imagen:** 233103\_i29  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| Plataforma de virtualización de red *VMware* NSX  Plataforma de virtualización de red de pila completa que cuenta con segmentación de red y microsegmentación para la carga de trabajo individual. (DELL, 2022). | | **Imagen:** 233103\_i30  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| DELL *SafeGuard and Response*  Permite prevenir amenazas desconocidas y responde en forma rápida y eficiente a los ataques ocultos en terminales, redes y nubes, con la ayuda de *VMware* *Carbon* *Black Cloud* y *Secureworks*. (DELL, 2022). | | **Imagen:** 233103\_i31  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| Arquitectura resistente cibernética de *PowerEdge*  Logra sobrepasar continuamente los límites del diseño de servidores reforzado para detectar los ataques cibernéticos y protegerse y recuperarse de ellos. (DELL, 2022). | | **Imagen:** 233103\_i32  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| DELL *SafeBIOS* y *SafeID*  Mitiga el riesgo de manipulación del BIOS con la detección de ataques de *firmware* integrada; utiliza el exclusivo chip de seguridad dedicado de DELL para mejorar la autenticación multifactor. (DELL, 2022). | | **Imagen:** 233103\_i33  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |
| DELL *Trusted Devices*  Dado que el 70 % de las infracciones se originan en el terminal, un ecosistema seguro comienza con *Dell Trusted Devices.* (DELL, 2022). | | **Imagen:** 233103\_i34  <https://media.istockphoto.com/vectors/cyber-security-line-icons-set-vector-illustration-editable-stroke-vector-id1338003094?k=20&m=1338003094&s=612x612&w=0&h=Bl6fS1Rk0LKRbSQmnCuqn-hGfPcRaiayQpz3iOMZRTk=> |

| Cuadro de texto |
| --- |
| Manual *Ransomware Defender* para Dell EMC *PowerScale*  Si desea profundizar sobre la herramienta *Ransomware Defender* para Dell EMC *PowerScale*, remítase al manual adjunto como Anexo 1.  **Descargar** |

| Cuadro de texto |
| --- |
| **Manual VMware NSX**  Para conocer un poco más sobre la plataforma de virtualización de red *VMware* NSX, ver el Anexo 2, que contiene el manual de uso.  **Descargar** |

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Para la Unión Europea, la violación en la seguridad de la información se origina cuando los datos quedan expuestos a incidentes de seguridad y repercute en la vulneración de la integridad, transparencia, disponibilidad y confidencialidad de los datos. Al ocurrir esto se ponen en riesgo los derechos y la privacidad de los dueños de la información, por lo que se debe notificar a las autoridades competentes en un plazo no mayor a 72 horas después de haber ocurrido el evento (Comisión Europea, s.f.). Dentro del siguiente tema se describen los aspectos asociados a la notificación de respuestas.  vulnerabilidad de seguridad log4j - antivirus fotografías e imágenes de stock  **Imagen:** 233103\_i35 | |

**2.2 Notificación de respuestas**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| La vulneración de la seguridad de la información implica un alto riesgo para los dueños de los datos, por lo tanto, deberán ser notificados de que esta ha sido violada y las medidas que ha tomado el responsable del tratamiento de los datos.  La notificación de respuesta de incidentes genera acciones de forma sistemática, con el objetivo de disminuir la ocurrencia y lograr una rápida recuperación, minimizando el daño causado a los servicios de la organización.  cerrar la ingeniería informática escribiendo código de programación en la base de datos en el teclado de la computadora portátil para proteger y bloquear el correo electrónico no deseado de internet y los piratas informáticos para el concepto de tec - antivirus fotografías e imágenes de stock  **Imagen:** 233103\_i36 | |

| **Tipo de recurso** | Slider Presentación | |
| --- | --- | --- |
| **Introducción** | A continuación, se describe la notificación de respuestas a incidentes extraída del Manual de Seguridad y Privacidad de la Información elaborado por el Ministerio de las Tecnologías de la Información y la Comunicaciones –MINTIC (2016). | |
| Notificar al primer punto de contacto  Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo al primer punto de contacto definido por la entidad (Ej.: Soporte de primer nivel). Esto se puede hacer a través de cualquier canal de comunicación (telefónico, correo, aplicativo, etc.). Es importante resaltar que debe existir un formato que el usuario debe diligenciar con la mayor cantidad posible de información relacionada. | | mujeres expertas en ciberseguridad que trabajan en la protección de la empresa - antivirus fotografías e imágenes de stock  **Imagen:** 233103\_i37 |
| Identificación del tipo de incidente  El primer punto de contacto identificará el tipo de incidente (de acuerdo a la tabla de clasificación que realiza la entidad), analizará si corresponde a un incidente de seguridad de la información o si está relacionado con requerimientos propios de la infraestructura de TI. En caso de ser catalogado como un incidente de seguridad, se notificará a la persona encargada de la atención, o a quien haga sus veces, para que tome las decisiones correspondientes. | | advertencia abstracta de un programa de malware detectado - antivirus fotografías e imágenes de stock  **Imagen:** 233103\_i38 |
| Esta será la encargada de realizar el seguimiento hasta su cierre definitivo. Si el incidente de seguridad es identificado por otra línea diferente a un usuario de la entidad, a través de los elementos de detección o administradores de TI, este es notificado directamente al responsable, quien tomará las acciones necesarias.  Se informará al primer punto de contacto sobre la presentación de un incidente de seguridad para que realice la documentación respectiva y esté atento al seguimiento y desarrollo de este. | | hombre actualizando un antivirus para evitar un hack - antivirus fotografías e imágenes de stock  **Imagen:** 233103\_i39 |
| Punto de contacto clave  El punto de contacto clave dentro de la gestión de incidentes es la persona encargada de la atención de estos, quien coordinará y asignará las actividades con las partes interesadas. Estos últimos solicitarán el apoyo a los involucrados en el proceso, con el fin de realizar la correcta ejecución de actividades que den solución al incidente. La persona encargada tendrá la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de una situación de este tipo y notificará a las altas directivas de la entidad. | | cerradura. concepto de datos - antivirus fotografías e imágenes de stock  **Imagen:** 233103\_i40 |

**SÍNTESIS**

| **Tipo de recurso** | Síntesis |
| --- | --- |
| Control de la seguridad digital  Síntesis: | |
| **Introducción** | Como refuerzo, a continuación encontrará la síntesis del componente formativo de una forma gráfica, así podrá repasar las diferentes temáticas tratadas. |
| **Nota:** elaboración propia del experto  **Imagen:** 233103\_i41  **Texto para diseñador web**  Seguridad informática  Evento  Situación que al presentarse denota una posible vulneración  Los eventos se monitorean  Plataforma  Notificación de respuestas  Incidente  Suceso no deseado y no planeado que puede causar daño  Los incidentes se validan  **CSIRT**  Equipo con la función de prestar los servicios que permiten prevenir y dar respuesta a incidentes  **CERT**  Equipo para dar respuestas a las emergencias informáticas  CENTRO DE GESTIÓN DE INCIDENTES | |

**Relación de conceptos**

| **Tipo de recurso** | Actividad didáctica. Arrastrar y soltar | |
| --- | --- | --- |
| Llegó el momento de validar los aprendizajes adquiridos con el estudio del componente formativo.  Por favor relacionar cada término con la definición, arrastrando y soltando donde corresponda. | | ilustraciones, imágenes clip art, dibujos animados e iconos de stock de vector isométrica de un trabajo en equipo diseño de nuevo software para proteger datos personales - equipo seguridad informatica  **Imagen:** 233103\_i42 |
| CERT | | Opera como un socio con el gobierno y la industria en el cumplimiento de la Ley y el mundo académico, con el fin de mejorar la seguridad y la capacidad de recuperación de los sistemas y redes informáticos |
| ColCERT | | Equipo coordinador a nivel nacional en aspectos de seguridad informática, el cual será el encargado de apoyar y colaborar con las demás instituciones a nivel nacional |
| Ciclo de gestión de incidentes | | Preparación, detección, análisis y notificación. |
| CSIRTS | | Pueden ser internos o externos, cubriendo áreas para manejo de incidentes en los centros de coordinación y análisis, además de los equipos de vendedores y proveedores. |
| Impacto de incidentes de seguridad | | Se verifica la aplicabilidad de las políticas de seguridad de la información. |
| Masificación de las TIC | | Aumento de los ataques e incidentes de seguridad de la información como, por ejemplo, manipulación de redes de datos, alteración de cajeros electrónicos y transferencias bancarias, generando pérdidas por billones de pesos. |
| Monitoreo continuo de equipos | | Hacen parte de la red de seguridad de la información, siguiendo unos protocolos o procedimientos descritos en la normatividad ISO 27000. Estos procedimientos deben ser establecidos o personalizados de acuerdo al tipo y necesidad de la empresa. |

RESULTADOS:

**>= 5/7** – FELICITACIONES – Tiene claro los conceptos básicos de la validación de incidentes, CSIRT, CERT y monitoreo de eventos.

**< 5/7** – Estimado aprendiz, es importante repasar nuevamente el contenido del componente formativo, los conceptos de validación de Incidentes, CSIRT, CERT, gestión de incidentes, plataformas de seguridad y notificación de respuestas, ya que no se ha comprendido en su totalidad.

**MATERIAL COMPLEMENTARIO**

| Tipo de recurso | Material complementario | | |
| --- | --- | --- | --- |
| Tema | Referencia APA del material | tipo | Enlace |
| CCENT/CCNA ICND1 100 - 105 : *official cert guide* | Wendell, O. (2016) *CCENT/CCNA ICND1 100 - 105: official cert guide.* Cisco Systems. | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000106585> |
| Estrategia de ciberseguridad para la sociedad digital. | Núñez Jarrosay, L. (2021) Estrategia de ciberseguridad para la sociedad digital. *Telemática.* 20 (1). P. 47-53 | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_doaj_primary_oai_doaj_org_article_f492659b81964e40aa0cfa17afaf7b25> |
| Propuesta de infraestructura técnica de seguridad para un equipo de respuesta ante incidentes de seguridad (CSIRT). | Ramírez Luna H. E. & Mejía Miranda, J. (2015) Propuesta de infraestructura técnica de seguridad para un equipo de respuesta ante incidentes de seguridad (CSIRT). *ReCIBE.* *Revista electrónica de Computación, Informática, Biomédica y Electrónica* p. VI | Artículo | [https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN\_cdi\_doaj\_primary\_oai\_doaj\_org\_article\_2fb23d76e9204433a27a187b95886220](about:blank) |
| *Specialized CSIRT for Incident Response Management in Smart Grids* | Martins, R.J, Días Knob, L. A. Germano Da Silva, E. Araujo Wickboldt, J., Schaeffer-Filho, A., & Zambenedetti Granville, L. (2018) Specialized CSIRT for Incident Response Management in Smart Grids. *Journal of Network and Systems Management* 27 (1) p. 269-285. | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_proquest_journals_2030542969> |

**GLOSARIO**

| **Tipo de recurso** | **Glosario** |
| --- | --- |
| CERT (*Computer Emergency Response Team*) | equipo para dar respuesta a las emergencias informáticas. |
| Contención, erradicación y recuperación de gestión de incidentes | después de analizar y priorizar el incidente, se procede a contener sus consecuencias y propagación. Las acciones por implementar deben ser previamente analizadas en conjunto con el equipo de atención de incidentes. |
| CSIRT | equipo que tiene la función de prestar los servicios que permiten prevenir y dar respuesta a incidentes de seguridad de la información. Se encargan , generalmente, de cubrir un área específica en una entidad pública o privada. |
| Detección y análisis de gestión de incidentes | es fundamental mitigar el impacto de los incidentes por medio de acciones eficientes, logrando alertar a la entidad cada vez que exista una situación. Después que el incidente se haya gestionado se debe realizar un informe, detallando causas, costos y el paso a paso a seguir para cuando se presente a futuro. |
| Evento | es una ocurrencia que al presentarse denota una posible vulneración en las políticas de seguridad de la información (PSI) o fallas significativas en los protocolos de control. Los eventos pueden o no pueden ocurrir, sin embargo, se puede apreciar como incumplimientos en la implementación de las PSI, o acciones sospechosas que pretenden sustraer información de los sistemas o aplicaciones. |
| Incidente | suceso no deseado y no planeado que puede causar daño. Según la norma ISO 27035 ‘Gestión de incidentes de SI’, se describe como un evento o serie de eventos de SI inesperados, que tienen una alta probabilidad de comprometer o interrumpir la operatividad de la entidad o empresa amenazando y afectando la transparencia, confidencialidad, disponibilidad e integridad de la información, o los equipos que la almacenan y gestionan. |
| Preparación de gestión de incidentes | se intenta minimizar la cantidad de incidentes mediante la aplicación de controles basados en resultados de evaluación de riesgos. Es importante tener presente que hay una cierta cantidad de incidentes que no pueden ser tratados, estos se denominan residuales. |
| Recolección y manejo de evidencias en gestión de incidentes | la recolección de evidencia y su posterior manejo debe realizarse con personal altamente entrenado y capacitado para llevar a cabo dichas acciones. La recolección de información es fundamental para iniciar procesos judiciales contra los atacantes, pero debe ser reunida cumpliendo estándares y recomendaciones legales, de acuerdo al procedimiento estipulado por la entidad. |
| Servicios en gestión de calidad de SI | dan valor agregado a los servicios reactivos y proactivos, además de ser complementarios a las buenas prácticas existentes en otros sectores, como las Tecnologías de la Información (TI), auditorías o áreas de capacitación. |
| Servicios proactivos | son aquellos que se presentan antes de ocurrir un suceso, llamados también servicios preventivos. Estos se anticipan a los eventos e incidentes protegiendo y asegurando los activos de la información. |
| Servicios reactivos | son los que se inician cuando el incidente ya ocurrió, es decir, un equipo de oficina comprometido o infectado, intrusos en registros de información, *malware* disperso por toda la red, *software* vulnerado o eventos identificados sin mecanismo previos de protección. |

**7**

**REFERENTES BIBLIOGRÁFICOS**

| **Tipo de recurso** | Bibliografía |
| --- | --- |
| Carnegie Mellon University (2022) *The CERT Division*. <https://www.sei.cmu.edu/about/divisions/cert/> | |
| Comisión Europea (s.f.) *¿Qué es una violación de la seguridad de los datos y qué deberíamos hacer en caso de sufrir una?* <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_es#:~:text=Una%20violaci%C3%B3n%20de%20la%20seguridad%20de%20los%20datos%20se%20produce,o%20integridad%20de%20los%20datos> | |
| Consejo Nacional de Política Económica y Social –CONPES-, República de Colombia & Departamento de Planeación –DNP- (2011) Lineamientos de Política para Ciberseguridad y Ciberdefensa. | |
| Heide der Van, M. (2020) *Estableciendo un CSIRT.* | |
| DELL (2022) *Soluciones de seguridad destacadas para las principales amenazas actuales.* <https://www.dell.com/es-co/dt/solutions/security/index.htm?gacd=10017601-14052-5761040-342546571-0&dgc=ST&gclid=Cj0KCQjwhY-aBhCUARIsALNIC041EsUQV8wdaADw7UR04_aIRZrbdh9DIRjuQjsWgziI0Z4-Y14q9lgaAma0EALw_wcB&gclsrc=aw.ds> | |
| Instituto para la Economía Social -IPES (2017) Gestión de incidentes de seguridad de la información. | |
| Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado ‘de la protección de la información y de los datos’ - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Enero 5 de 2009. DO N° 47223. | |
| Martins, R.J, Días Knob, L. A. Germano Da Silva, E. Araujo Wickboldt, J., Schaeffer-Filho, A., & Zambenedetti Granville, L. (2018) Specialized CSIRT for Incident Response Management in Smart Grids. *Journal of Network and Systems Management* 27 (1) p. 269-285. | |
| Ministerio de las Tecnologías de la Información y la Comunicaciones –MINTIC (2016). Guía N° 21. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. | |
| Núñez Jarrosay, L. (2021) Estrategia de ciberseguridad para la sociedad digital. *Telemática.* 20 (1). P. 47-53 | |
| Ramírez Luna H. E. & Mejía Miranda, J. (2015) Propuesta de infraestructura técnica de seguridad para un equipo de respuesta ante incidentes de seguridad (CSIRT). *ReCIBE.* *Revista electrónica de Computación, Informática, Biomédica y Electrónica* p. VI | |
| Wendell, O. (2016) *CCENT/CCNA ICND1 100 - 105: official cert guide.* Cisco Systems. | |

# **CONTROL DEL DOCUMENTO**

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

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

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