**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Tratamiento de riesgos de ciberseguridad en la micro, pequeña y mediana empresa (*mipyme*) |
| --- | --- |

| COMPETENCIA | 220501111 - Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-03 - Hacer tratamiento de incidentes de seguridad digital para MiPymes de acuerdo con resultado del monitoreo, estándares y normatividad vigente. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 06 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Tratamiento de los incidentes de seguridad de la información |
| BREVE DESCRIPCIÓN | La gestión de incidentes de seguridad de la información se consolida como estrategias para atender en un mínimo tiempo cualquier evento que ponga en riesgo la seguridad de la misma, a partir de la aplicación de métodos y técnicas para identificar, evaluar, atender y recuperar, garantizando así la continuidad del negocio. |
| PALABRAS CLAVE | Evaluación, identificación, incidente, recuperación, registro |

| ÁREA OCUPACIONAL | 2 - CIENCIAS NATURALES, APLICADAS Y RELACIONADAS |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**

**Introducción**

1. **Evaluación de la seguridad digital**
   1. Gestión de vulnerabilidades
   2. Tipos de pruebas
   3. *Hacking* ético
   4. Equipos de seguridad *RedTeam & BlueTeam*
2. **Gestión de incidentes de seguridad digital** 
   1. Normatividad relacionada
   2. Aplicación
   3. Características
   4. Documentación

**Síntesis**

1. **INTRODUCCIÓN**

Las organizaciones se enfrentan a diario a gran variedad de amenazas que ponen en riesgo sus activos de información más preciados y que son necesarios para dar continuidad al negocio, que en algunas ocasiones se vuelve una actividad de tipo “bombero” en la que se busca atender y dar respuesta sin lineamientos o unas instrucciones claras, que permitan establecer planes para atender otros incidentes que surjan en el futuro, aprovechando las vulnerabilidades presentes o alguna otra que sea nueva. El siguiente video presenta la importancia de la gestión de incidentes y la profundización que se tendrá de esta temática a lo largo del componente:

| CF06\_Video\_Introducción |
| --- |

1. **DESARROLLO DE CONTENIDOS**
2. **Evaluación de la seguridad digital**

| A medida que las organizaciones van implementando soluciones y estrategias articuladas para la gestión de la ciberseguridad en las organizaciones, se hace necesario que esta sea evaluada para determinar si está siendo efectiva y si no se están aprovechando otras vulnerabilidades, que no han sido identificadas o se estén generando nuevas brechas a la seguridad de la información. | Dispositivo protegido por ciberseguridad |
| --- | --- |

Las normas como la familia ISO 27000 y *frameworks* técnicos como NIST han incorporado dentro de su metodología las fases que llevan a que las estrategias sean evaluadas de tal manera que permita identificar debilidades y a partir de estas establecer nuevos focos de la estrategia de seguridad, teniendo como premisa, que este ejercicio debe ser permanente y continuo, debido a que las amenazas crecen de manera permanente y cada vez son más complejas.

A continuación, se reconocen algunas técnicas que permiten realizar una evaluación de la seguridad digital en las organizaciones y que son el insumo fundamental para determinar la efectividad y eficiencia de la estrategia propuesta:

* 1. **Gestión de vulnerabilidades**

Este ejercicio de gestionar las vulnerabilidades, que pueden ser aprovechadas para convertirse en una amenaza para una organización, es un trabajo complejo dependiendo el tamaño de la organización y de la cantidad de sus activos de información (es decir cada uno de los recursos de información útil para la organización, así como los que indirectamente son necesarios para que ese dato o información pueda funcionar) tal como se observa la caracterización de dichos tipos de activos de información en la siguiente figura:

**Figura 1**

*Activos de información*



| Los ejercicios para la gestión de vulnerabilidades pueden variar de acuerdo al tipo de organización y el enfoque que se le quiera dar a la gestión; pues es muy distinto realizar una gestión de vulnerabilidades en una institución financiera o crítica frente a una pequeña o mediana empresa. |
| --- |

El procedimiento para su desarrollo ha sido basado en siete etapas principales que abordan esta gestión, entre las que se encuentran:

| CF06\_1\_1\_Infografía Interactiva\_etapas |
| --- |

A partir de estas etapas anteriormente descritas, han surgido diferentes alternativas para este ejercicio, como se puede apreciar en la siguiente figura:

**Figura 2**

*Metodologías para la gestión de vulnerabilidades*

| CF06\_1\_1\_Infografía\_metodologías |
| --- |

De las cuales se profundizará en algunas de ellas:

***NIST*.** Este marco de trabajo para la mejora de la seguridad cibernética en infraestructuras críticas, el cual fue generado por el Gobierno de los Estados Unidos a mediados del año 2014, brinda a las organizaciones la metodología para la reducción de riesgos cibernéticos a partir de una adecuada gestión de riesgos.

Este marco de trabajo, propone la gestión desde una serie de funciones, las cuales se desarrollan de manera simultánea y continua como son: **Identificar, Proteger, Detectar, Responder** y **Recuperar.** Estas funciones del marco de trabajo, conlleva a desarrollar una serie de actividades basadas en categorías, encaminadas a reducir los riesgos que se pueden presentar y afectar la información de una organización. A continuación, se puede observar un resumen de estas categorías y actividades que se desarrollan para la adecuada gestión de vulnerabilidades:

| CF06\_1\_1\_Infografía Interactiva\_funciones |
| --- |

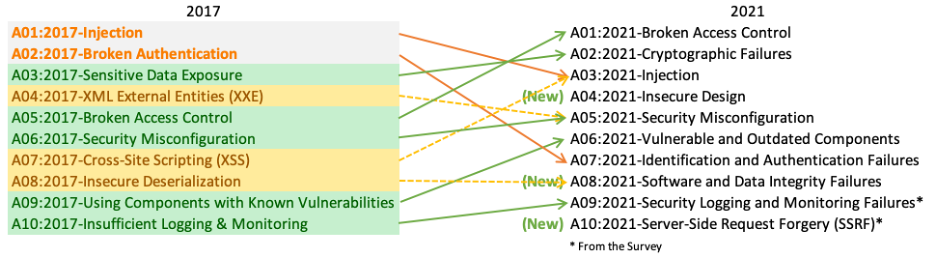
| *NIST*  Aunque este ha sido propuesto para infraestructuras críticas, se puede aplicar a cualquier tipo de organización, lo que lo hace un método muy llamativo para entidades del gobierno. Consulte la versión completa del documento desde su sitio oficial. Este recurso también está en el material complementario. | Ir al sitio web |
| --- | --- |

***OWASP*.** Es una organización sin fines lucrativos, la cual busca ayudar a visibilizar las vulnerabilidades en aplicaciones para su mejoramiento de la seguridad a partir de una adecuada gestión del riesgo, siendo este un pilar fundamental para el desarrollo y aplicación de su metodología.

*Owasp* provee de un *framework* abierto el cual permite implementar auditorías en aplicaciones principalmente de tipo web, basados esencialmente en pruebas de caja blanca y caja negra. A partir de su ejercicio identifica las vulnerabilidades más representativas y presentes en la actualidad en su *Owasp* *top* 10. En su último reporte, el *Owasp Top* 10 2021 se puede apreciar la siguiente clasificación frente al informe previo del año 2017:

**Figura 3**

*Owasp Top 10 2021*



Nota: Tomado de OWASP (2021)

Con base en este reporte, se analiza el comportamiento de las vulnerabilidades identificadas, así:

| CF06\_1\_1\_pestañas verticales\_comportamiento |
| --- |

| OWASP  Dado lo anterior, *owasp*, se ha vuelto una metodología práctica para la identificación de vulnerabilidades en las aplicaciones *web* más utilizadas por los equipos de desarrollo en los últimos años. Se sugiere explorar y hacer uso de esta metodología, consultando su documento oficial. Este recurso también está en el material complementario. | Ir al sitio web |
| --- | --- |

***ISSAF*.** Es un marco de trabajo para el testeo e identificación de vulnerabilidades de seguridad estructurado en tres fases. Esta metodología está enfocada en realizar análisis de seguridad a partir de los resultados obtenidos, a continuación, se observa un esquema general de sus fases y su respectiva conceptualización:

| CF06\_1\_1\_Infografía\_fases de ISSAF |
| --- |

| *ISSAF*  Este proyecto lleva varios años sin mantenimiento, pero se puede consultar el texto completo de la metodología en el enlace. Este recurso también puede ser consultado en el material complementario. | Ir al sitio web |
| --- | --- |

***OSSTMM*.** Esta metodología para pruebas de seguridad también es muy utilizada y, debido a su aplicación tan extensa, se ha convertido en un estándar de facto para el desarrollo de auditorías de seguridad, ya que proporciona un marco de trabajo que describe las actividades a desarrollar, las cuales están comprendidas como se presentan a continuación:

**Tabla 1**

*Secciones y revisiones de la metodología OSSTMM 2.1*

| SECCIÓN | REVISIÓN |
| --- | --- |
| Sección A -Seguridad de la Información | Revisión de la Inteligencia Competitiva |
| Revisión de Privacidad |
| Recolección de Documentos |
| Sección B - Seguridad de los Procesos | Testeo de Solicitud |
| Testeo de Sugerencia Dirigida |
| Testeo de las Personas Confiables |
| Sección C - Seguridad en las tecnologías de Internet | Logística y Controles |
| Exploración de Red |
| Identificación de los Servicios del Sistema |
| Búsqueda de Información Competitiva |
| Revisión de Privacidad |
| Obtención de Documentos |
| Búsqueda y Verificación de Vulnerabilidades |
| Testeo de Aplicaciones de Internet |
| Enrutamiento |
| Testeo de Sistemas Confiados |
| Testeo de Control de Acceso |
| Testeo de Sistema de Detección de Intrusos |
| Testeo de Medidas de Contingencia |
| Descifrado de Contraseñas |
| Testeo de Denegación de Servicios |
| Evaluación de Políticas de Seguridad |
| Sección D - Seguridad en las Comunicaciones | Testeo de PBX |
| Testeo del Correo de Voz |
| Revisión del FAX |
| Testeo del Modem |
| Sección E - Seguridad Inalámbrica | Verificación de Radiación Electromagnética (EMR) |
| Verificación de Redes Inalámbricas [802.11] |
| Verificación de Redes Bluetooth |
| Verificación de Dispositivos de Entrada Inalámbricos |
| Verificación de Dispositivos de Mano Inalámbricos |
| Verificación de Comunicaciones sin Cable |
| Verificación de Dispositivos de Vigilancia Inalámbricos |
| Verificación de Dispositivos de Transacción Inalámbricos |
| Verificación de RFID |
| Verificación de Sistemas Infrarrojos |
| Revisión de Privacidad |
| Sección F - Seguridad Física | Revisión de Perímetro |
| Revisión de monitoreo |
| Evaluación de Controles de Acceso |
| Revisión de Respuesta de Alarmas |
| Revisión de Ubicación |
| Revisión de Entorno |

Nota. Adaptado de ISECOM (2021)

| *OSSTMM*  Si se desea profundizar detalles de esta metodología, se puede consultar su sitio oficial; el cual también se encuentra ubicado en el material complementario. | Ir al sitio web |
| --- | --- |

**PTES.** Se consolida como estándar para pruebas de penetración y *testing*, que puede ser aplicado en cualquier organización. Entre sus objetivos se encuentra el de disponer de un marco de trabajo para la realización de auditorías técnicas de seguridad en sistemas de información. Se desarrolla en las siguientes siete fases:

| CF06\_1\_1\_Infografía\_fases de PTES |
| --- |

| *PTES*  Su consulta para conocer más a detalle esta metodología puede ser a través de su sitio oficial, el cual también se encuentra en el material complementario. | Ir al sitio web |
| --- | --- |

Las metodologías anteriormente descritas permitirán realizar un análisis de vulnerabilidades, establecer planes de acciones y un proceso importante, que es adoptar planes de mejoramiento al interior, dado que el proceso de gestión de vulnerabilidades debe ser un proceso continuo.

* 1. **Tipos de pruebas**

Cuando se está desarrollando el proceso de evaluación de la seguridad, se debe de garantizar que los resultados presentados estén respaldados en ejercicios de verificación y comprobación que permitan establecer si una condición se está cumplimento o no; para este caso estamos hablando de controles, técnicas, tácticas para el aseguramiento de la información y en este ejercicio pueden surgir diferentes alternativas para verificar este tipo de cumplimientos, entre las que se pueden apreciar:

| CF06\_1\_2\_tarjetas con número\_alternativas |
| --- |

Existen varios tipos de pruebas que se pueden realizar a las aplicaciones o soluciones con las que cuenta la organización que permite verificar si realmente están realizando las operaciones según lo solicitado y lo establecido en el programa.

Su aplicación dependerá del alcance de la evaluación a realizar, así como también dependerá si las soluciones son construidas *in-house* o son adquiridas a un tercero, en cualquiera de los casos, debería de validarse la información para garantizar su integridad

* 1. ***Hacking* ético**

El *hacking* ético o también denominado sombrero blanco, es un conjunto de técnicas que se aplican para el descubrimiento de vulnerabilidades dentro de un entorno o un conjunto de aplicaciones.

Esta técnica se desarrolla de manera consentida y aprobada por las organizaciones y los responsables de realizar las validaciones correspondientes, con lo cual buscan identificar las debilidades, anormalidades y falencias en su seguridad.

Los expertos que realizan este tipo de validaciones hacen uso de técnicas especializadas que se denominan Test de Penetración o *Pentesting*, y su objetivo es burlar los controles de seguridad y en caso de conseguir una identificación positiva, este deberá reportarlo a la organización. Este tipo de estrategia no debería de causar daño, dado que es concebido y tiene fines de exploración.

Este ejercicio se desarrolla básicamente en las siguientes 5 fases:

**Figura 4**

*Fases del hacking ético*

| CF06\_1\_3\_Infografía\_fases |
| --- |

Ahora bien, dependiendo de su alcance, se puede determinar el tipo de *hacker* requerido, tal como se evidencia:

| CF06\_1\_3\_Infografía\_interactiva\_tipo de hacker |
| --- |

Estos ejercicios son muy comunes cuando las organizaciones quieren identificar vulnerabilidades presentes en sus sistemas, y requieren que una persona externa desarrolle esta actividad, pero siempre mediando algún acuerdo de confidencialidad y naturalmente una autorización de por medio.

* 1. **Equipos de seguridad *Red Team & Blue Team***

Los equipos de seguridad *Red Team & Blue Team* se consolidan como estrategias para organizaciones más complejas y de mayor tamaño y como su nombre lo indica, está conformado por equipos de personas quienes, desde cada uno de sus grupos, realizan acciones para la identificación de vulnerabilidades.

Este concepto proviene de elementos relacionados con entrenamiento militar, los cuales fueron adoptados por la disciplina de la ciberseguridad y que incorporaron para establecer estrategias de auditoría desde dos frentes distintos. Veamos:

| CF06\_1\_4\_Infografía\_equipos de seguridad |
| --- |

Entre algunas actividades que desarrollan los equipos se encuentran:

| CF06\_1\_4\_Acordeón\_actividades de los equipos |
| --- |

Sumado a lo anterior, contar con estos equipos en las organizaciones puede fortalecer a la empresa a través de estos beneficios:

| CF06\_1\_4\_Infografía\_beneficios |
| --- |



1. **Gestión de incidentes de seguridad digital**

| Actualmente, la gestión de incidentes se establece en las organizaciones como una capacidad para hacer frente a los diferentes requerimientos e incidentes que se presentan cada día, desarrollando actividades enmarcadas en buenas prácticas buscando regresar las operaciones de la organización a su estado normal en un tiempo mínimo. | Male and Female Programmers Talking about Work, Solving Problems Together, Using Laptop Computer. Software Development / Code Writing / Website Design / Database Architecture Concept |
| --- | --- |

Esta tendencia de apropiar los procedimientos para la gestión de incidentes busca que las organizaciones cuenten cada día con estrategias para afrontar de una manera muy rápida y casi que sistemática a su estado normal de operaciones, reduciendo el tiempo fuera de línea o reduciendo pérdida de activos de información.

Antes de dar paso a las temáticas asociadas, es importante tener clara la definición del término incidente y es que de acuerdo a la Norma ISO-IEC 27035:2012. Un incidente de seguridad de la información se define como:

| “*Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazas la seguridad informática*” (ICONTEC, 2012) |
| --- |

Con este concepto claro, vamos ahora a revisar algunos aspectos importantes para la adopción de un modelo de gestión de incidentes:

* 1. **Normatividad relacionada**

Como todo procedimiento tecnológico que está regulado, la gestión de incidentes se fundamenta en estándares para la atención y remediación de los incidentes que se pueden presentar en una organización; es así como se encuentran los siguientes referentes interesantes:

* GTC-ISO-IEC 27035:2012 - Gestión de incidentes de seguridad de la información
* NIST SP 800-61 Rev. 2- Guía de manejo de incidentes de seguridad informática

A continuación, se explica cada uno de estos:

**GTC-ISO-IEC 27035:2012 - Gestión de incidentes de seguridad de la información**

Esta norma técnica es una de las principales que existe actualmente y sirve como base para el establecimiento de otras normas y marcos de trabajo para la gestión de incidentes de seguridad informática. Proporciona los lineamientos necesarios para la adopción en una organización y prepararse para atender cualquier tipo de incidente.

Además, se vincula con las estrategias de seguridad de las organizaciones para la implementación de controles y procedimientos que posibiliten la continuidad del negocio reduciendo el impacto por alguna amenaza materializada. Sugiere cinco fases establecidas para la gestión de los incidentes de seguridad, como se enumeran a continuación:

| CF06\_2\_1\_Infografía\_interactiva\_fases de gestión |
| --- |

| Esta norma es de las más adoptadas por las organizaciones, ya que su modelo permite su fácil adopción y alineación con sistemas de gestión como los SGSI. |
| --- |

**NIST SP 800-61 Rev. 2- Guía de manejo de incidentes de seguridad informática**

El Instituto Nacional de Normas y Tecnología NIST nos hace entrega de la guía de incidentes para seguridad informática, la cual dicta los lineamientos para la gestión de la seguridad de la información de acuerdo a su correspondiente análisis y metodología de evaluación.

Esta guía en su metodología también propone unas fases para la atención de incidentes de seguridad, como se puede apreciar en su esquema de ciclo de vida:

| CF06\_2\_1\_Infografía\_interactiva\_fases ciclo de vida |
| --- |

| Este guía para la gestión de incidentes también ha cobrado fuerza entre las organizaciones, por su fácil aplicabilidad y por la aplicabilidad incluso de terceros de la organización. |
| --- |

* 1. **Aplicación**

Desde el punto de vista metodológico y para las organizaciones colombianas, el MinTIC, ha generado una guía para la adopción de estos planes en las organizaciones tanto públicas principalmente pero no excluye las entidades privadas. Esta guía se denomina “*Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*” y establece los lineamientos para su adopción de acuerdo al siguiente esquema:

| CF06\_2\_2\_pasos verticales\_proceso de gestión |
| --- |

La guía brinda así mismo, las indicaciones para su adopción en la organización, definiendo los recursos humanos, económicos y de procedimiento, necesarios para su implementación y operación, en donde se ha involucrado el *Csirt* Gobierno, como entidad que acompaña dicho proceso a las entidades gubernamentales.

| Gestión y Clasificación de Incidentes de Seguridad  Se sugiere consultar este documento base desde el sitio oficial del MinTIC para conocer los detalles y guía de implementación. Este recurso se encuentra también en el material complementario. | Ver documento |
| --- | --- |

* 1. **Características**

La gestión de incidentes desde lo establecido por la guía del MinTIC, se aborda desde cada una de sus fases, estableciendo las características y condiciones para su adopción y desarrollo de las actividades enmarcadas en el plan. En este orden de ideas, se recorrerá cada una de las fases sugeridas, para reconocer sus características, funciones y actividades:

| CF06\_2\_3\_Infografía\_fases caracteristicas |
| --- |

Veamos una explicación de cada una:

* **Preparación**

Esta fase conlleva a que las entidades establezcan el plan para afrontar un incidente de seguridad. Esto involucra fortalecer las capacidades de detección, evaluación, contención y/o recuperación. Esta fase debe estar directamente apoyada por las áreas responsables de tecnología, dado que deben de reconocer las capacidades actuales y las necesarias para realizar una adecuada gestión.

Dentro de las actividades que deben adelantar para la preparación, se recomiendan:

| CF06\_2\_3\_Infografía\_preparación |
| --- |

* **Detección, evaluación y análisis**

Esta fase requiere que la organización fortalezca las capacidades para detectar, evaluar y analizar cualquier comportamiento por fuera de lo común; para ello, se recomienda:

| CF06\_2\_3\_slide con títulos\_detecc\_eva\_ana |
| --- |

A continuación, se presenta un ejemplo de una escala de prioridad en la actividad de priorización de los incidentes y tiempos de respuesta:

**Tabla 1**

*Ejemplo de niveles de criticidad de impacto*

| Nivel criticidad | Valor | Definición |
| --- | --- | --- |
| Inferior | 0.10 | Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas. |
| Bajo | 0.25 | Sistemas que apoyan a una sola dependencia o proceso de una entidad. |
| Medio | 0.50 | Sistemas que apoyan más de una dependencia o proceso de la entidad. |
| Alto | 0.75 | Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas. |
| Superior | 1.00 | Sistemas Críticos |

Nota. Tomado de MinTIC (2021)

Ahora bien, de acuerdo con el impacto futuro, este dependerá del daño que pueda causar si no es contenido y se representa a continuación:

**Tabla *2***

*Ejemplo de niveles de impacto actual y futuro*

| Nivel impacto | Valor | Definición |
| --- | --- | --- |
| Inferior | 0.10 | Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| Bajo | 0.25 | Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| Medio | 0.50 | Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo |
| Alto | 0.75 | Impacto moderado en uno o más componentes de más de un sistema de información. |
| Superior | 1.00 | Impacto alto en uno o más componentes de más de un sistema de información. |

Nota. Tomado de MinTIC (2021)

* **Contención erradicación y recuperación**

Esta fase es de gran importancia, ya que incorpora la estrategia propuesta para tomar decisiones en caso de presentarse un incidente y evitar que este se propague o tenga una mayor afectación. Consta de los siguientes componentes:

| CF06\_2\_3\_Tarjetas conectadas\_componentes |
| --- |

* **Actividades post-incidentes**

Esta fase se desarrolla posterior a la recuperación tras un incidente y busca consolidar los informes que con los detalles más precisos que informen la situación presentada.Entre ellas se encuentran las lecciones aprendidas, las cuales hacen parte del plan de mejoramiento continuo, buscando conocer en detalle lo sucedido, sus vectores de ataque, soluciones dadas y plan de erradicación y recuperación para ocasiones futuras.

* 1. **Documentación**

La gestión de incidentes, como parte primordial de las estrategias de seguridad de la información en las organizaciones, se fundamenta en la información recolectada, la cual es fundamental para la toma de decisiones, informes, lecciones aprendidas e incluso para el mejoramiento continuo del plan de gestión.

En este orden de ideas, se debe mantener un registro detallado de los incidentes de seguridad que son identificados, para poder dar tratamiento y una gestión adecuada. Se empieza estableciendo los mecanismos de captura de estos incidentes, para lo cual puede ser útil documentos de captura, o formularios que recolectan la información relevante, la norma GTC-ISO-IEC 27035:2012 en su anexo D, presenta algunos modelos de formularios que pueden ser adaptados a nuestras necesidades. Algunos de ellos son:

| CF06\_2\_4\_interactivo\_procesos de documentación |
| --- |

| Formulario GTC-ISO-IEC 27035:2012  En la norma anteriormente citada, se pueden encontrar múltiples modelos de formularios, los cuales pueden ser adaptados a las necesidades de la organización. Por otra parte, a continuación, se puede observar un modelo de formulario básico para la captura de información de un incidente. Esta información, dado que almacenará datos personales, estará obligada a contar con los procesos necesarios para la protección adecuada de datos y garantizar así su privacidad. | Ver imagen |
| --- | --- |

**D. SÍNTESIS**

Contar con una estrategia de seguridad digital que permita hacer frente a cualquier evento que ponga en riesgo la seguridad de la información y reduzca el riesgo de no continuar con el desarrollo de las actividades propias del negocio, hoy en día, es de gran importancia. Las normas técnicas y guías de implementación permitirán establecer las estrategias, condiciones y procedimientos necesarios para hacer frente a eventos que afecten el normal desarrollo de las actividades de la organización.

Es así como se estudió que entre las normas que más se ajusta a las necesidades actuales están la GTC-ISO-IEC 27035:2012, la cual, además de ser una de las más usadas en las grandes organizaciones, ha servido como referente para otros marcos, validando así su aplicabilidad a cualquier industria.

El siguiente esquema permite visualizar de manera genérica lo aquí expuesto:

| CF06\_esquema\_síntesis |
| --- |

**E. ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Gestión de incidentes de seguridad de la información. |
| Objetivo de la actividad | Comprender la implementación de un plan de gestión de incidentes de seguridad en una organización a través del reconocimiento de sus fases. |
| Tipo de actividad sugerida | Relación de términos |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Actividad didáctica 1 - CF06 |

**F. MATERIAL COMPLEMENTARIO**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del recurso o  archivo del documento o material |
| --- | --- | --- | --- |
| 1. Evaluación de la seguridad digital | Chifla-Villón, M., Puma-Aucapiña, L. & Villacís-Real, K. (2020). Elaboración de un instrumento de auditoría que evalúa la seguridad lógica aplicable en servidores en Instituciones Públicas de Educación Superior de la Zona 5 del Ecuador. *Revista CIENCIA UNEMI*, 13(34), 127–143. | Artículo | <https://search-ebscohost-com.bdigital.sena.edu.co/login.aspx?direct=true&db=fap&AN=146126581&lang=es&site=ehost-live> |
| 1.1. Gestión de vulnerabilidades | Nist. (2022). *Framework Documents.* | Sitio web | <https://www.nist.gov/cyberframework/framework> |
| 1.1. Gestión de vulnerabilidades | OWASP. (2022). *WSTG – Stable*. | Sitio web | <https://owasp.org/www-project-web-security-testing-guide/stable/> |
| 1.1. Gestión de vulnerabilidades | OISGG. (2006). *Penetration Testing Framework* (PTF). | Libro | <http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf> |
| 1.1. Gestión de vulnerabilidades | Pentest-standard.org. (s.f.). *PTES Technical Guidelines.* | Sitio web | <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines> |
| 1.1. Gestión de vulnerabilidades | ISECOM. (2021). *OSSTMM*. | Sitio web | <https://www.isecom.org/research.html#content5-9d> |
| 1.3 Hacking ético | Rodríguez Llerena, A. E. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informatica Medica*, 12(1), 116–131. | Artículo | <https://search-ebscohost-com.bdigital.sena.edu.co/login.aspx?direct=true&db=fap&AN=144392670&lang=es&site=ehost-live> |
| 2. Gestión de incidentes de seguridad digital | ICONTEC. (2012). *Gtc-iso-iec 27035:2012 tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información*. | Norma técnica | <https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=311> |
| 2.1. Normatividad relacionada | MinTIC. (2021). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.* | Guía | <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237908_maestro_mspi.pdf> |

**G. GLOSARIO**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Contención | Proceso mediante el cual se busca evitar que un incidente se propague o genere una mayor afectación. |
| Detección | Fase en la cual se identifican eventos que posiblemente pueden afectar la seguridad de la información |
| Incidente | “Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazas la seguridad informática” (ICONTEC, 2012) |
| ISIRT | Equipo de respuesta a incidentes de seguridad de la información. |
| Recuperación | Proceso que busca restablecer los servicios o activos a su estado normal. |

**H. REFERENCIAS BIBLIOGRÁFICAS**

ISECOM. (2021). *OSSTMM*. <https://www.isecom.org/research.html#content5-9d>

MinTIC. (2021). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237908_maestro_mspi.pdf>

OISGG. (2006). *Penetration Testing Framework* (PTF). <http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf>

OWASP. (2021). *Welcome to the OWASP Top 10 – 2021*. <https://owasp.org/Top10/>

**I. CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Hernando José Peña Hidalgo | Experto Temático | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Octubre de 2022 |
| Miroslava González Hernández | Diseñadora Instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Octubre de 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital – Centro de Diseño y Metrología | Octubre de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Octubre de 2022 |
| Sandra Patricia Hoyos Sepúlveda | Corrección de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Octubre de 2022 |

**J. CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

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