**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Herramientas tecnológicas para la planeación estratégica, riesgo y cumplimiento. |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica | RESULTADOS DE APRENDIZAJE | 220501108-01 - Realizar la valoración de riesgos de ciberseguridad acorde parámetros de referencia y normatividad vigente. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 06 |
| NOMBRE DEL COMPONENTE FORMATIVO | Evaluación de la seguridad de la información en organizaciones |
| BREVE DESCRIPCIÓN | La seguridad de la información en las organizaciones es un proceso que se sugiere, todas deben realizarlo con el fin de evaluar las estrategias adoptadas para la gestión de las vulnerabilidades y que estas no puedan afectarla, generando incidentes que pueden terminar en hechos más complejos para la misma organización. |
| PALABRAS CLAVE | Auditoria, *Bug*, indicador, prueba, vulnerabilidad |

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

1. **TABLA DE CONTENIDOS:**

**Introducción**

1. **Gestión de vulnerabilidades**
   1. Metodologías
   2. Herramientas
   3. Activos de información
   4. Técnicas de recolección de información
2. **Evaluación de la seguridad de la información**
   1. Establecimiento del alcance
   2. Identificación de activos
   3. Identificación de vulnerabilidades
   4. Identificación de amenazas
   5. Establecimiento de salvaguardas
   6. Evaluación del riesgo
   7. Tratamiento del riesgo
3. **INTRODUCCIÓN**

Un factor importante que deben tener presente hoy en día las organizaciones, es estar un paso adelante de cualquier situación que ponga en riesgo sus activos de información, es por eso que adoptar procesos de evaluación de la seguridad de la información de manera permanente, permite recolectar información importante para la aplicación de acciones correctivas en su infraestructura tecnológica, sistemas de información e incluso ajuste en sus procedimientos operativos en donde se ubican las personas que operan los sistemas, pero que lastimosamente suelen ser el factor más débil de la cadena de a ciberseguridad.

Video introducción

CF06\_video\_indtroducción

En el presente componente formativo, se identifican las metodologías y como se evalúa la información obtenida, para establecer un nivel de seguridad de la información en la organización.

1. **DESARROLLO DE CONTENIDOS:**
2. **Gestión de vulnerabilidades**

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en un componente esencial para el funcionamiento efectivo de las organizaciones. La gestión de vulnerabilidades se erige como una práctica crucial en este contexto, ya que permite identificar, evaluar y mitigar los riesgos asociados a las amenazas cibernéticas que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos y sistemas de una entidad.

Por otra parte, la gestión de las vulnerabilidades es un proceso, visto desde la óptica de la ciberseguridad, el cual debe de realizarse de manera permanente y con el que se busca identificar aquellas fragilidades que pueden afectar a los activos de información de una organización, estos ejercicios serán primordiales para mejorar los niveles de seguridad, dado que permite a partir de un proceso evaluativo, identificar los puntos fuertes que deben de mantenerse, así como los puntos débiles en los cuales debe trabajar la organización.

A continuación, se reconoce un poco mejor estos procedimientos.

* 1. **Metodologías**

Gestionar las vulnerabilidades que pueden convertirse en una amenaza para una organización, es un trabajo complejo que requiere identificar, clasificar, priorizar y resolver las vulnerabilidades o debilidades dentro de los sistemas operativos, aplicaciones empresariales, aplicaciones de usuario final y navegadores web de una organización. La complejidad de este proceso depende del tamaño de la organización y de la cantidad de sus activos de información. En la siguiente figura se caracterizan dichos activos de información.

**Figura 1**

*Activos de información*



Nota: adaptado de <https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf>

Los ejercicios para la gestión de vulnerabilidades pueden ser varios, de acuerdo al tipo de organización y el enfoque que se le quiera dar a la gestión, 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 7 etapas principales que abordan esta gestión, como se presentan en la figura 2, entre los que se encuentran:

**Figura 2**

*Etapas generales de la gestión de vulnerabilidades*

**Etapas generales de la gestión de vulnerabilidades:
Planeación:
Definición de activos
Planeación de la evaluación 
Descubrimiento:
Recopilación de Información
Mapeo de elementos
Análisis y evaluación del riesgo:
Identificación de brechas
Determinar impacto
Definición de plan de acción:
Diseño plan de mitigación
Determina controles
Ejecución de Plan de acción:
Implementa controles y acciones
Verificación de la efectividad:
Verifica planes y acciones
Lecciones aprendidas:
Revaluar y mejorar el proceso de gestión de vulnerabilidades**

Nota: adaptado de <https://www.b-secure.co/recursos/infografias/proceso-de-gestion-de-vulnerabilidades-seguridad>

Dicho procedimiento, junto con cada una de las etapas, se explica a continuación:

Slide\_simple

CF06\_1.1\_ Etapas\_gestión\_vulnerabilidades\_formato\_

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

**Figura 3**

*Metodologías para la gestión de vulnerabilidades*

En la figura se tienen los sitios oficiales de:
NIST National Institute of Standards and Technology:
Instituto Nacional de Estándares y Tecnología (nist.gov)
OWASP Open Web Aplication Security Projects:
OWASP Foundation, la base de código abierto para la seguridad de las aplicaciones | Fundación OWASP
ISSAF Information Systems Security Assesment
www.oissg.org 
OSSTMM Open Source Security Testing Methodology
OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad - DragonJAR
PTES Penetratiion Testing Excecution Standard
El estándar de ejecución de pruebas de penetración (pentest-standard.org)
WASC-TC Web Aplication Security Consortium Threat Classification
El Consorcio de Seguridad de Aplicaciones Web / Clasificación de Amenazas (webappsec.org)

Nota: Imágenes tomadas de sitios oficiales.

De las cuales vamos a reconocer algunas de ellas:

**NIST- Instituto Nacional de Estándares y Tecnología**: este marco de trabajo para la mejora de la seguridad cibernética en infraestructuras críticas, el cual ha sido 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.

Así mismo, propone la gestión desde una serie de funciones, las cuales se desarrollan de manera simultánea y continua: **identificar, proteger, detectar, responder** y **recuperar,** como se puede observar en la siguiente figura:

**Figura 4**

*Framework (infraestructura) de NIST*

Nota: tomado de <https://www.nist.gov/cyberframework>

Estas funciones del marco de trabajo, conlleva 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.

**Tabla 1**

*Funciones del framework de NIST*

| **FUNCIÓN IDENTIFICADOR ÚNICO** | **FUNCIONES** | **CATEGORÍA IDENTIFICADOR ÚNICO** | **CATEGORÍAS** |
| --- | --- | --- | --- |
| **ID** | IDENTIFICADOR | ID.AM  ID.BE  ID.GV  ID.RA  ID.RM  ID.SC | Gestión de activos.  Ambiente de negocios  Gobernanza.  Evaluación de riesgos.  Estrategia de gestión de riesgo.  Gestión del riesgo de la cadena de suministros. |
| **PR** | PROTEGER | PR.AC  PR.AT  PR.DS  PR.IP  PR.MA  PR.OPT | Gestión de identidad, autenticación y control de acceso.  Conciencia y capacitación.  Seguridad de datos.  Procesos y procedimientos de protección de la información.  Mantenimiento.  Tecnología de protección. |
| **DE** | DETECTAR | DE.AE  DE.CM  DE.DP | Anomalías y eventos.  Monitoreo continuo de seguridad.  Procesos de detección. |
| **RS** | RESPONDER | RS.RP  RS.CO  RS.AN  RS.MI  RS.IM | Planificación de respuesta.  Comunicaciones.  Análisis.  Mitigación.  Mejoras. |
| **RC** | RECUPERAR | RC.RP  RC.IM  RC.CO | Planificación de recuperación.  Mejoras.  Comunicaciones. |

Nota: Adaptado de https://www.nist.gov/cyberframework

Aunque este ha sido propuesto para infraestructuras críticas, se puede observar que es aplicable a cualquier tipo de organización, lo que lo hace un método muy llamativo para entidades del gobierno, en material complementario se puede consultar la versión completa del documento desde su sitio oficial.

**OWASP*-*** ***Open Web Application Security Project***: organización sin fines lucrativos, la cual busca ayudar a visibilizar las vulnerabilidades en aplicaciones para el 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 *framework* abierto el cual permite aplicar auditorías en aplicaciones en especial de tipo web, basados principalmente en pruebas de caja blanca y caja negra y a partir de su ejercicio identificar las vulnerabilidades más representativas y presentes en la actualidad en su Owasp top 10.

Lo anterior permite generar reportes sobre las vulnerabilidades que más se encuentran en las aplicaciones web, en su reporte el *Owasp* *Top* 10 2021, se puede apreciar la clasificación frente al informe previo del año 2017, consultando en material complementario de esta guía.

En este reporte se observa el comportamiento de las vulnerabilidades identificadas, teniendo en cuenta:

Pestañas verticales

CF06\_1.1\_OWASP

Dado lo anterior, Owasp, se ha vuelto una metodología práctica para la identificación de vulnerabilidades en las aplicaciones web más utilizada por los equipos de desarrollo en los últimos años; quienes quieran explorar y hacer uso de esta metodología, en el material complementario se puede consultar su documento oficial.

**ISSAF-** ***Information Systems Security Assessment Framework***: este marco de trabajo para el testeo e identificación de vulnerabilidades de seguridad, la cual está estructurada en 3 fases como son:

* **Planeación y preparación**: la cual establece los pasos iniciales para el desarrollo de la auditoría y ejercicios de testeo.

Entre las actividades relacionadas se encuentran: identificación de interesados, reuniones de apertura, definición de enfoque y metodología y cronograma de tiempo.

* **Evaluación**: en esta fase, se desarrollan las validaciones de acuerdo a las siguientes 9 capas:
  + Recolección de información.
  + Mapeo de la red de trabajo.
  + Identificación de vulnerabilidades.
  + Penetración.
  + Obtención de acceso y escalamiento de privilegios.
  + Enumeración.
  + Compromiso de usuarios y sitios remotos.
  + Mantener el acceso.
  + Cubrir rastros.
* **Reportes, limpieza y destrucción de objetos**: fase donde se analizan las pruebas, se consolidan resultados y se presentan los reportes a los interesados

Esta metodología está enfocada en realizar análisis de seguridad a partir de los resultados obtenidos, a continuación, podemos observar un esquema general de sus fases. Se puede consultar en material complementario la metodología ISSAF.

***OSSTMM*-** ***Open Source Security Testing Methodology Manual***: 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 2**

*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 <https://www.isecom.org/>

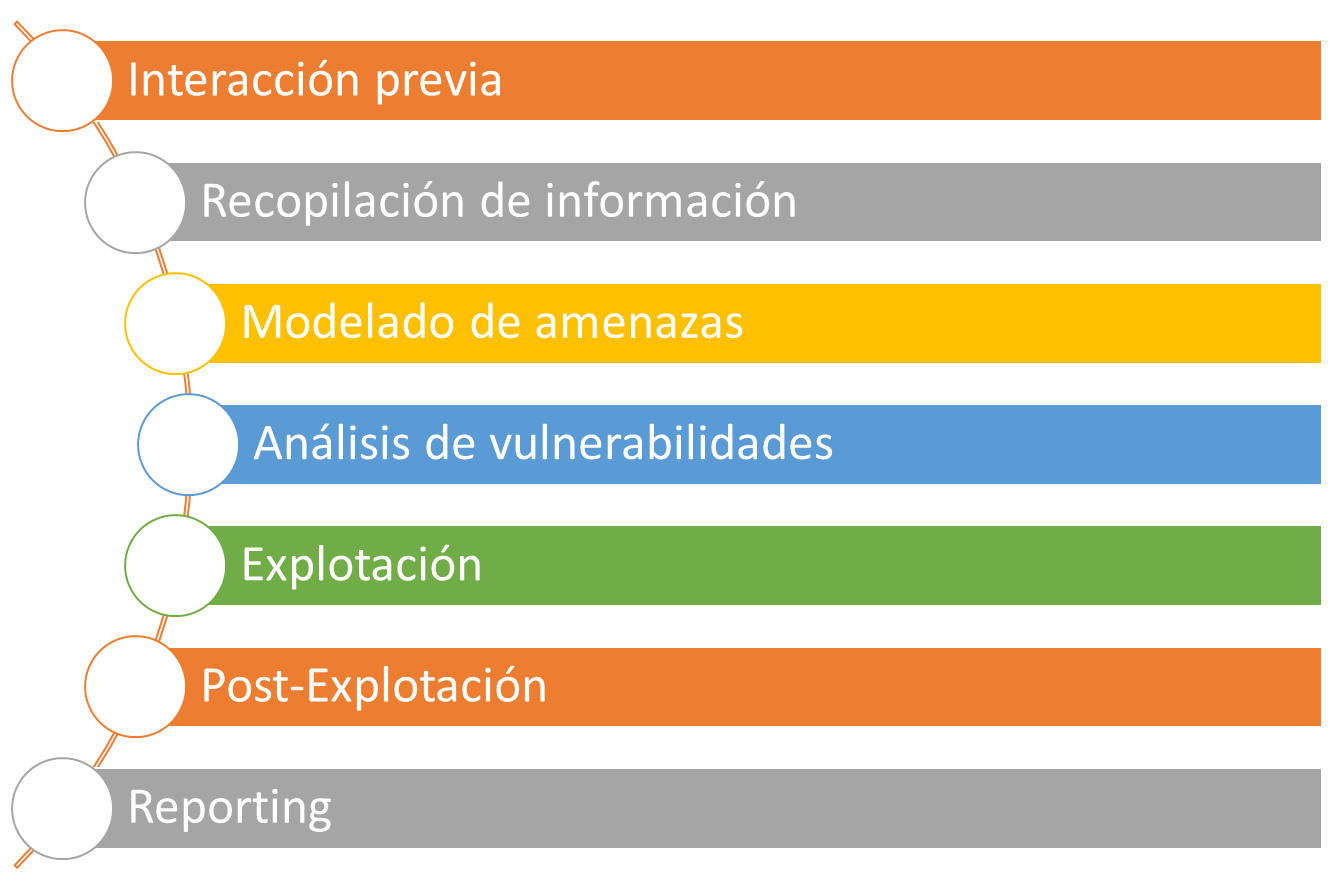
Detalles de esta metodología, pueden ser consultados en material complementario.

**PTES- *Penetration Testing Execution Standard***: se consolida como estándar para pruebas de penetración y *testing* y 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 7 fases, como se presenta en la siguiente figura:

**Figura 5**

*Fases de la metodología PTES*



Nota: adaptado de <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines>

Esta metodología puede ser consultada en material complementario.

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

* 1. **Herramientas**

Los procedimientos a desarrollar en la búsqueda de vulnerabilidades, puede ser un proceso engorroso y en muchas ocasiones demorado, dado la cantidad de revisiones y validaciones que se deben realizar por cada uno de los activos de información que existen en la organización, es aquí donde podemos apoyar este ejercicio con herramientas especializadas que permitan buscar y evaluar las vulnerabilidades de manera sistemática o automatizada.

En este aspecto se encuentra una amplia gama de posibilidades, algunas de tipo comercial, así como *open* *source* que pueden ser muy útiles para el desarrollo de estas actividades, a continuación, se reconocen algunas de estas herramientas, se resaltan sus beneficios y capacidades para el desarrollo de este ejercicio de búsqueda.

Slide de imágenes

CF06\_1.2\_Herramientas\_slide\_imagenes

Las anteriores son tan solo una muestra pequeña de la gran cantidad de herramientas disponibles para el desarrollo de ejercicios de evaluación de la seguridad en sistemas de información de las organizaciones, y es importante reconocer que aunque la mayoría de estas herramientas son bajo licencia comercial dado la funcionalidad, beneficios, tableros de control integraciones y reportes, también hay herramientas de tipo open *source* distribuidas para evaluación, pero se recomienda primero antes de aplicarlo en un entorno de producción, verificar que estas no presenten algún riesgo para la información como perdidas, eliminación o corrupción.

A continuación, se comparte un listado de herramientas útiles que pueden ser utilizadas en entornos de producción, siempre y cuando sean obtenidas en su sitio oficial o desde alguno de sus sitios de publicación.

**Tabla 3**

*Otras herramientas útiles para la evaluación de seguridad*

|  |  |  |
| --- | --- | --- |
| *Nombre herramieta* | *Nombre herramienta* | *Nombre herramienta* |
| *Nexpose* | *Nikto* | *Tripwire IP360* |
| *Wireshark* | *Aircrack-NG* | *Retina CS* |
| *Microsoft Baseline Security Analyzer* | *Secunia Personal Software Inspector* | *Probely* |
| *Vulnerability Manager Plus* | *Nmap* | *Metasploit* |
| *Veracode* | *Nipper Studio* | *GFI LanGuard* |
| *Core Impact* | *Qualys* | *SAINT* |
| *Safe3WVS* | *WebReaver* | *AVDS* |
| *AppScan* | *Clair* | *OWASP Zed Attack Proxy (ZAP)* |
| *Burp Suite* | *SqlMap* | *Muchas más* |

Estas herramientas permitirán realizar una gran cantidad de pruebas, de manera rápida, además de presentar los resultados en informes enriquecidos, que permitirá tomar decisiones para la gestión de la seguridad en una organización.

* 1. **Activos de información**

Antes de iniciar con los ejercicios de evaluación, es importante que se tenga claridad sobre cuáles serán los activos de información que se evaluarán, y en cuáles deberá presentar una gran atención, es por ellos que reconocer los activos, permite en primer lugar, reconocer la importancia para la organización, así como establecer la herramienta y técnica a utilizar para su evaluación.

De acuerdo a la “**Guía para la Gestión y Clasificación de Activos de Información**”, de MinTic (2016), las organizaciones deberían de realizar un reconocimiento y clasificación de sus activos de información, con el fin de ser utilizados en los diferentes ejercicios de evaluación de seguridad, este reconocimiento busca primordialmente:

* Identificar los activos de la organización, esta identificación busca el reconocimiento de los aspectos básicos del activo como: nombre, observación, proceso al cual sirve, propietario, custodio, personas a las cuales tienen acceso y qué tipo de acceso, entre otros.
* Identificar el propietario de la información.
* Mantener una clasificación de acuerdo a su valor para la organización, la criticidad, la susceptibilidad y en función a su responsabilidad legal.
* Establecer un etiquetado de la información, que permita identificar claramente el activo por cualquier integrante de la organización.

Para lo cual se recomienda estructurar la información de la siguiente manera:

* **Identificador**: código único dentro de la organización y que identifica únicamente un activo de información.
* **Proceso**: proceso o procesos a los cuales pertenece el activo de información.
* **Nombre activo**: nombre del activo de información.
* **Descripción/Observación**: descripción o notas que se consideren importantes para identificar en el activo.
* **Tipo**: establece el tipo de recurso, entre los cuales se pueden utilizar: información, *software*, recurso humano, servicio, *hardware*, otros.
* **Ubicación**: ubicación tanto física como electrónica donde se almacena el activo de información.
* **Clasificación**: hace referencia a la protección de información de acuerdo a confidencialidad, integridad y disponibilidad.
* **Justificación**: establece para cada valoración el impacto que causaría una afectación del activo.
* **Criticidad**: valor general del activo para la organización, la cual puede ser: alta, media o baja.
* **Propietario**: persona u organización responsable de suministrar los datos.
* **Custodio**: persona o proceso responsable por tratar y custodiar la información en la organización.
* **Acceso**: usuarios o procesos que deberían tener acceso, especificando el tipo de acceso.
* **Fecha de ingreso y salida del activo**: fechas en las cuales ha sido utilizado un activo de información.

Una vez se haya reconocido estos activos, y para el ejercicio de evaluación de seguridad, es necesario el reconocimiento de la infraestructura tecnológica, aplicaciones y demás elementos que la conforman para realizar la evaluación, en este caso será necesario reconocer:

* Producto.
* Versión.
* Arquitectura.
* Marca.
* Modelo.
* Último mantenimiento.
* Estado de garantías.
* Cláusulas de contrato de mantenimiento.
* Última actualización.
* Responsable.
* Ubicación.

Entre otros aspectos.

Esta información, permitirá reconocer la información que deberá ser evaluada, así como los sistemas de información que serán objetos de auditoría.

* 1. **Técnicas de recolección de información**

Contar con insumos verídicos y reales para la evaluación de la seguridad de la información, es primordial para obtener un resultado confiable, es por ello que se debe hacer uso de una o varias técnicas que permitan corroborar la verificación propuesta.

Tabs\_horizontales

CF06\_1.4\_Técnicas de recolección de información\_

Dependiendo del activo de información y de la validación a realizar, el auditor puede seleccionar la técnica que más se ajuste y permita recolectar la información necesaria para establecer un resultado confiable.

1. **Evaluación de la seguridad de la información**

La evaluación de la seguridad de la información es un proceso crítico en la gestión de datos y sistemas en la era digital. Su objetivo principal es identificar y mitigar posibles vulnerabilidades que podrían comprometer la confidencialidad, integridad y disponibilidad de la información. Mediante la realización de auditorías, pruebas de penetración y análisis exhaustivos, las organizaciones pueden evaluar la eficacia de sus medidas de seguridad existentes y tomar decisiones informadas para mejorar su postura de seguridad. La evaluación de la seguridad de la información es esencial en un mundo donde las amenazas cibernéticas son cada vez más sofisticadas e invasivas, garantizando así la protección de datos sensibles y la continuidad de las operaciones empresariales en un entorno digital en constante evolución.

Evaluar la seguridad de la información en una organización, es un ejercicio que debe tomarse con responsabilidad y pertinencia hacia la organización, ya que de esta evaluación permitirá confrontar si se está en capacidad de hacer frente a una situación que ponga en riesgo la seguridad de su información, así como el normal desarrollo de sus actividades.

A continuación, se revisará el procedimiento para llevar a cabo la evaluación técnica de la seguridad de la información en una organización.

* 1. **Establecimiento del alcance**

Para llevar a cabo la evaluación de la seguridad de la información, es preciso tener definido el alcance de esta, lo que permitirá establecer hasta donde llegará o cual será el objeto de la evaluación dentro de la organización, teniendo presente que se está hablando de una evaluación de seguridad de la información, será necesario evaluar como mínimo los activos que comprenden los procesos, áreas o dependencias que involucran la evaluación, de estos activos, se debe levantar la siguiente información:

* Procesos, dependencias o áreas de la organización a la cual se desea evaluar.
* Activos de información objeto de evaluación.
* Información.
* *Software*.
* *Hardware*.
* Personal.
* Infraestructura de red.
* Sedes o ubicaciones de la organización.
* Y todos aquellos elementos que se consideren que intervienen en los procesos de la compañía.

Además, se debe establecer hasta donde se quiere llegar con la evaluación de seguridad, es decir, si está pensando en reconocer sus vulnerabilidades o está planeando la adquisición de alguna solución de seguridad o la subcontratación de la misma.

Algo que se debe de indagar, es si previamente se ha realizado algún proceso de evaluación, lo que permitirá tener un panorama previo y verificar su validez y trayectoria de las vulnerabilidades.

* 1. **Identificación de activos**

Una vez definido el alcance, se debe realizar la identificación y reconocimiento de los activos que serán objeto de evaluación, también conocer quien o quienes son los responsables de cada uno de estos activos al interior de la organización, para lo cual se recomienda un levantamiento de información que permita identificar a cada uno de estos actores dentro de la organización, a continuación, se tiene un ejemplo de cómo se puede documentar esta información.

**Tabla 4**

*Modelo levantamiento de información sobre activos a evaluar*

|  |  |  |
| --- | --- | --- |
| Tipo Activo | Activo | Responsable |
| *Software* | Aplicación talento humano | Pedro Pérez – Talento humano |
| Financiero | Juan de la Oz – Contador |
| Información | Información de clientes | Juan Muñoz – Comercial |
| *Hardware* | Servidor de base de datos | Carlos Aranda – Sistemas |
| Redes wifi | Carlos Aranda – Sistemas |

Esta información, debe ser documentada a partir del procedimiento del reconocimiento de los activos de información que se realiza inicialmente en la organización, así como en una exploración más en detalle con cada una de las áreas o procesos responsables de la información, lo que permitirá identificar otros aspectos objeto de evaluación.

Como se mencionó anteriormente sobre activos de información, se permitirá aprovechar la información recolectada para obtener los detalles de cada uno de los activos a evaluar, tales como versión, marca, arquitectura, modelo, entre otros detalles, además del establecimiento de la importancia para la organización de cada uno de estos activos.

* 1. **Identificación de vulnerabilidades**

Las amenazas se consideran cualquier debilidad o falencia que puede presentarse en un activo de información, que está presente y que podría ser aprovechada por un tercero, es así como la identificación de estas de manera temprana, permite establecer un plan de evaluación para su identificación, como se vio anteriormente hay algunas iniciativas como la del [*Top* 10 de *Owasp*](#bookmark=id.gjdgxs), el cual consolida las 10 vulnerabilidades más comunes en aplicaciones web, entre las que se destacan:

* Ausencia o debilidad de controles de seguridad.
* Sistemas de información desactualizados que facilitan la explotación.
* Diseño de aplicaciones complejas y poco intuitivas, que conllevan al error por parte del usuario.
* Falta de políticas y controles para la gestión adecuada de credenciales de acceso.
* Falta de controles para medios de almacenamiento removibles.
* Ausencia de controles para riesgos eléctricos.
* Medios de conexión deficientes o sin control, que permite que cualquier intruso pueda acceder a la red de datos o aplicaciones.
* Sistemas de información implementados con un dimensionamiento inadecuado generando sobrecostos o fallas en operación.
* Ausencia de políticas para la gestión del cambio.
* Información clasificada erróneamente.
* Mecanismos de respaldo y recuperación ineficientes.
* Debilidad en la seguridad física y de perímetro.
* Falta de formación del personal encargado y usuarios finales.
* *Software* instalado no autorizado o de dudosa reputación.
* Falta de evaluación de *software*.
* Falta de políticas y controles para el acceso remoto.
* Falta de control sobre los datos de entrada y de salida.
* Falta de documentación de la infraestructura tecnológica.
* Falta de auditorías o desarrollo débil de las mismas.
* Procedimientos para limpieza de desechos tecnológicos débil o ausentes.
* Sistemas de identificación y autenticación débiles.
* Descargas e instalaciones de aplicaciones de internet.
* Conexiones a redes públicas desprotegidas.
* Falta de cultura y compromiso para el de trabajo seguro.

Todas estas vulnerabilidades y muchas más pueden estar presentes en los activos de información de la organización sin darse cuenta, podrían ser la entrada para que una amenaza aproveche y se pueda materializar.

Su reconocimiento **NO** debe hacerse de manera general, sino por cada uno de los activos y valorar sus dimensiones, permitiendo caracterizarlas y realizar la evaluación acertada.

* 1. **Identificación de amenazas**

Con las vulnerabilidades identificadas, es preciso que el reconocimiento de amenazas se realice, a partir de la validación de posibilidades de ocurrencia y del impacto que pueden generar en cada uno de los activos de información, como se dijo anteriormente, esta identificación no debe realizarse de manera general sino individual por cada activo de información.

Las amenazas pueden ser establecidas a partir de recomendaciones como lo hace *Magerit*, en la cual sugiere la siguiente clasificación:

Acordeón

CF06\_2.4\_Amenazas sugeridas por Magerit\_

Estas amenazas permitirán reconocer que puede afectar a la organización, a partir del aprovechamiento de las vulnerabilidades anteriormente identificadas, y su valoración del impacto será determinante para el siguiente paso, que será el establecimiento de la salvaguarda adecuada.

* 1. **Establecimiento de salvaguardas**

El siguiente paso es el establecimiento de las salvaguardas o controles, como también, acciones que deberá de aplicar la organización para evitar que una vulnerabilidad sea aprovechada, para ello, se tienen iniciativas existentes como la norma ISO/IEC 27001 Anexo A, el cual presenta algunos controles importantes para mejorar la seguridad de la información, como son los controles CIS:

* **Norma ISO/IEC 27001 Anexo A**: esta norma presenta las propuestas de controles, representada en dominios de seguridad, los cuales permiten abarcar los diferentes frentes de un activo de información (ICONTEC, 2018).

A continuación, se presentan los dominios de seguridad sugeridos por la norma:

**Figura 6**

*Dominios de seguridad de la norma ISO/IEC 27001:2013*



Nota: Adaptada de ISO/IEC 27001:2013 – Anexo A pp. 23. <https://serviciocivil.gov.co/sites/default/files/marco-legal/2006_03_22_NTC-ISO-IEC%2027001.pdf>

Estos dominios adicionalmente están distribuidos en objetivos de control, los cuales agrupan los distintos enfoques de seguridad y finalmente los controles, tal como se tiene en el componente formativo “Gestión del riesgo en las organizaciones”, del presente programa.

* **Controles CIS**: es una propuesta de código abierto realizada por un grupo o comunidad de profesionales y organizaciones que trabajan en el ámbito de la ciberseguridad. Esta norma propone 18 controles con los cuales se fortalece la infraestructura tecnológica, servicios y aplicaciones, con el fin de reducir la probabilidad de ocurrencia de un incidente (*CIS SECURITY*, 2022). En material complementario puede consultar su página oficial.

Los controles CIS, están estructurados en 18 controles y 153 salvaguardas distribuidos en 3 grupos de implementación, así:

**Figura 7**

*Controles CIS V8*

En la figura se observa los 18 controles para salvaguardas:
1. Inventario y control de los activos empresariales
2. Inventario y control de activos de software
3. protección de datos
4. Configuración segura de activos de software
5. Gestión de cuentas
6. Gestión del control de acceso
7. Gestión continua de vulnerabilidades
8. gestión de registgro de auditoria
9. Protección de correo electrónico y navegador web
10. Defensas contra el malware
11. Recuperación de datos
12. Gestión de la infraestructura de red
13. Supervisión y defensa de la red
14. Concientización y capacitación en materia de seguridad
15. Gestión de proveedores de servicios
16. Seguridad del software de aplicación
17. Gestión de respuesta a incidentes
18. Pruebas de penetración

Nota: adaptado de <https://blog.segu-info.com.ar/2023/04/controles-cis-esenciales-de.html>

Adicionalmente, cuenta con una recopilación de sugerencias específicas para productos, en los cuales adopta dichos controles, de acuerdo a las características de cada uno de los productos, generando guías de endurecimiento que facilita a los administradores de estos sistemas de información su adaptación.

Entre las guías más comunes se tienen las siguientes:

* Sistemas operativos *Linux* como *Windows*.
* Servicios web, bases de datos.
* Hipervisores.
* Servicios en la nube.
* Dispositivos móviles.
* Dispositivos de red.
* Software de escritorio.
* Dispositivos de impresión.

Para mayor información en material complementario se puede consultar el portal oficial.

Las salvaguardas seleccionadas deberán ser evaluadas para garantizar su aplicación y efectividad para la gestión de posibles riesgos de amenaza, en formatos como los presentados anteriormente del SoA.

En material complementario se ubica el enlace para descargar el formato en Excel, del registro de salvaguardar para la gestión del riesgo

* 1. **Evaluación del riesgo**

Las acciones adelantadas a partir del ejercicio de evaluación, deberán de reducir considerablemente las probabilidades de que las vulnerabilidades sean aprovechadas por las amenazas, y estas generen un incidente que lleve a la organización a un incidente que afecte sus operaciones, e incluso posibilite perder parte de su información, para garantizar que las acciones sean aplicadas adecuadamente, se debe realizar un plan de seguimiento o evaluación periódica, que permita reconocer la efectividad de las mismas (INCIBE, 2015).

Estas evaluaciones deben ser establecidas a partir de métricas y mediciones que permitan establecer el nivel de seguridad, las cuales deberán ser:

* **Métrica indirecta**: las cuales están destinadas a la mejora de la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, entre otros.
* **Métrica directa**: esta se centra en la velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, entre otros.

Para este caso en donde las métricas son para la medición de la seguridad, estas deben aplicarse a los controles propuestos e implementados anteriormente, lo que permitirá reconocer el grado de eficiencia de cada uno de ellos.

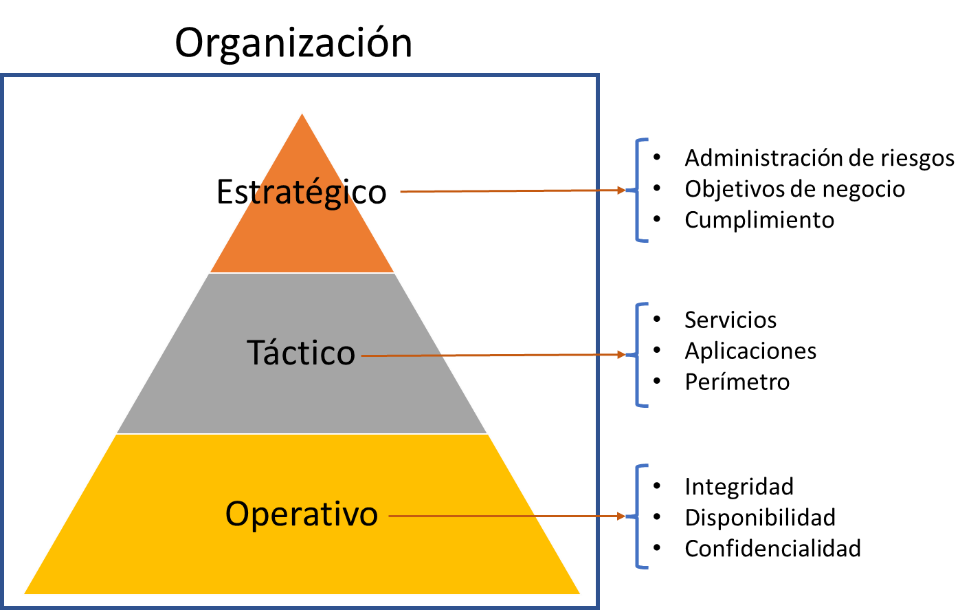
En el establecimiento de las métricas, se debe tener presente que:

* Deben ser alcanzables en un tiempo estimado.
* Debe ser expresadas en escalas de porcentaje o escalas numéricas.
* Deben explicar los componentes evaluados.
* Deben permitir identificar puntos débiles.
* Debe permitir conocer los riesgos a los que se enfrenta la organización.

La seguridad de la organización debe permitir evaluarse desde 3 niveles diferentes, como son: estratégico, táctico y operativo, como se muestra a continuación.

**Figura 8**

*Niveles de decisión de una organización*



A continuación, se presenta una descripción más detallada de cada nivel de decisión, desde lo estratégico, táctico y operativo:

Tabs\_verticales

CF06\_2.6\_Niveles decisión organización

La evaluación se deberá realizar a partir de un plan diseñado con este propósito, en donde se permita verificar la adecuada implementación, funcionamiento y pertinencia frente a las diferentes amenazas que presenta la organización.

Su aplicación deberá ser confrontada a través de diferentes ejercicios que demuestren la aplicabilidad y efectividad del control, algunas formas de aplicar la validación podrían ser:

* Cuestionarios.
* Inspección visual.
* Toma de notas.
* Comparación de datos de diferentes momentos.
* Muestreo.
* Consulta directa a sistemas de información.
* Prueba de penetración.
* Verificación de registros.

Y los resultados deberán ser documentados para el cálculo definitivo de la evaluación a través de instrumentos como hojas de cálculo, como las que propone el MinTIC en su hoja de evaluación de MSPI que se puede descargar en formato Excel en material complementario.

* 1. **Tratamiento del riesgo**

Finalmente, una vez obtenido una evaluación de la ciberseguridad aplicada a los activos de información, se debe establecer el plan de mejoramiento, que se traduce en el establecimiento de nuevas acciones y estrategias que deben de plantearse para continuar sosteniendo y mejorando la seguridad de la información en la organización.

Estos planes de mejoramiento deberán de incluir:

Slide\_simple

CF06\_2.7\_Tratamiento del riesgo\_

El desarrollo de este plan deberá ser revisado y aprobado por la dirección o responsable designado, quien presentará las mejoras propuestas.

El tratamiento del riesgo en las organizaciones es un proceso fundamental para garantizar su sostenibilidad y éxito a largo plazo. Implica la identificación, evaluación y posterior gestión de los riesgos que pueden afectar a la organización en sus diferentes dimensiones, desde la financiera hasta su reputación. Este enfoque proactivo permite a las organizaciones tomar decisiones informadas, implementar estrategias de mitigación y aprovechar oportunidades de manera más efectiva. Al abordar el tratamiento del riesgo de manera sistemática, las organizaciones pueden proteger sus activos, mejorar su resiliencia y mantener la confianza de sus partes interesadas, contribuyendo así a su crecimiento y éxito continuo.

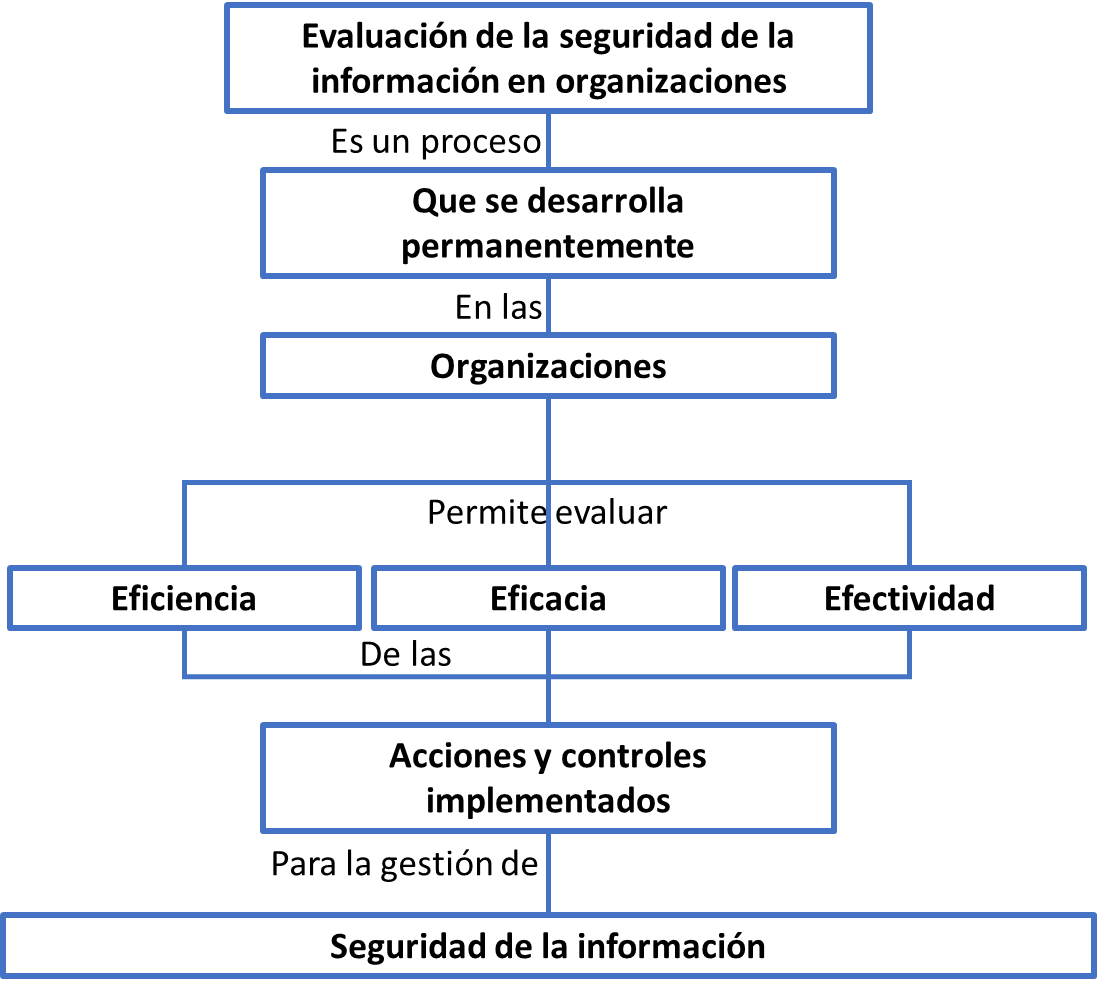
Es importante tener presente, que estos procesos para gestionar la seguridad, se deben hacer de forma permanente y continua, lo que sugiere que debe realizarse de manera periódica y sistemática, de tal modo que pueda identificarse puntos débiles y aplicar sus correctivos, favoreciendo la mejora continua.

1. **SÍNTESIS**

Evaluar y mantener la seguridad de la información en una organización es un proceso permanente, que debe realizarse en todas las organizaciones sin importar el tamaño, naturaleza o ubicación, dado que las amenazas pueden afectar los activos, buscando como aprovecharse de la falta de controles.

Estos procesos que aparentemente son complejos, hoy en día con la ayuda de las metodologías y las herramientas especializadas, permiten realizar estos ejercicios en pasos sencillos y sin complicaciones, además, brindan toda la información necesaria para tomar decisiones y establecer los planes necesarios para la gestión de las vulnerabilidades y amenazas.

Queda en manos de las mismas organizaciones destinar el recurso, tiempo y personal para realizarlo y así evitar pérdidas que afecten el desarrollo de las operaciones.



1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Cuestionario evaluación de la seguridad de la información en organizaciones |
| Objetivo de la actividad | Identificar los temas principales del componente formativo evaluación de la seguridad de la información en organizaciones. |
| Tipo de actividad sugerida | Cuestionario verdadero falso |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | CF06\_ActividadDidactica\_cuestionario |

1. **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 |
| 1.1 Metodologías | *NIST National Institute of Standards and Technology.* (2023). *CYBERSECURITY FRAMEWORK* | Web | <https://www.nist.gov/cyberframework/framework> |
| 1.1 Metodologías | *OWASP Open Web Aplication Security Projects.* (2023). *WSTG - Stable*. | Web | <https://owasp.org/www-project-web-security-testing-guide/stable/> |
| 1.1 Metodologías | *ISSAF*. (2006). *Information Systems Security Assesment Framework ISSAF Draft* 0.2.1 | Documento | <http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf> |
| 1.1 Metodologías | *ISECOM. OSSTMM Open Source Security Testing Methodology.* (s.f). *The open source security testing methodology manual*. | Documento | <https://www.isecom.org/OSSTMM.3.pdf> |
| 1.1 Metodologías | *PTES Penetration Testing Excecution Standard.* (2012). *PTES Technical Guidelines*. | Guía | <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines> |
| 1.1 Metodologías | *OWASP TOP 10. ¿Qué ha cambiado en el Top 10 para 2021?* | Web | <https://owasp.org/Top10/> |
| 1.1 Metodologías | *Metodología ISSAF. Approach & Methodology. Página 14.* | Web | <http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf> |
| 1.3. Activos de información | MinTIC. (2020). Instrumento de evaluación MSPI. | Hoja de cálculo | <https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx> |
| 2.5. Establecimiento de salvaguardas | *Center for Internet Security.* (2023). *CIS Critical Security Controls.* | Web | <https://www.cisecurity.org/controls> |
| 2.5. Establecimiento de salvaguardas | *Center for Internet Security.* (2023). *CIS Benchmarks List. Lista de puntos de referencia de la CIE* | Web | <https://www.cisecurity.org/cis-benchmarks/> |
| 2.5 Establecimiento de salvaguardas | Universidad Nacional de Colombia (2018). Guía técnica colombiana ISO 19011: 2018. | Libros digitales | <http://siga.unal.edu.co/images/Modulos/Ova/Capacitacion_Guia_tecnica_auditoria_NTC_ISO_19011_2018.pdf> |
| 2.5 Establecimiento de salvaguardas | Norma Internacional ISO 31000. (2018). Administración/ Gestión de riesgos – Lineamientos guía. | Libros digitales | https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486 |
| 2.5 Establecimiento de salvaguardas | ICONTEC (2018). NTC-ISO-IEC 27001:2013 – Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. | Libros digitales | https://serviciocivil.gov.co/sites/default/files/marco-legal/2006\_03\_22\_NTC-ISO-IEC%2027001.pdf |
| 2.5 Establecimiento de salvaguardas | Fernández Rivero, P. P. & Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. (pp 36-57). | Libros digitales | <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/53624?page=36> |
| 2.5 Establecimiento de salvaguardas | Formato registro de salvaguardar para la gestión del riesgo. | Hoja de cálculo | <https://f.hubspotusercontent30.net/hubfs/4444632/Declaraci%C3%B3n%20de%20aplicabilidad%20Excel%20-%20Anexo%20ISO%20270012013.xlsx> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| *Bug* | Error en un paquete *software* que puede generar fallos en el procesamiento de la información. |
| Evidencia | Conjunto de información que respaldan un hecho o evento. |
| Hallazgo de auditoría | Son los eventos o registros que sirven para reconocer si un control se está aplicando adecuadamente o no. |
| Indicador | Son unidades de medición que facilitan la evaluación de una acción realizada. |
| *Pentesting* | También llamado pruebas de penetración consiste en el conjunto de técnicas de acceso no autorizado a sistemas de información, con el fin de identificar posibles vulnerabilidades. |
| Registros | Conjunto de datos, que sirve para almacenar la información de un hecho, evento, persona u objeto. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

INCIBE (2017). Gestión de riesgos - Una guía de aproximación para el empresario. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf>

Instituto Nacional de Estándares y Tecnología. (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. <https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf>

ISO27001. (2020). Evaluación del desempeño en ISO 27001. <https://normaiso27001.es/evaluacion-del-desempeno-en-iso-27001/>

MINTIC. (2016). Seguridad y Privacidad de la Información - Guía de gestión de riesgos. <https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf>

OSSTMM 3. (2022). The Open Source Security Testing Methodology Manual.

<https://www.isecom.org/OSSTMM.3.pdf>

Tamayo Saborit, M. & González Capote, D. (2020). La gestión de riesgos: herramienta estratégica de gestión empresarial. Editorial Universo Sur. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/131885>

Tithink. (2015). Gestión de Riesgos Magerit. <https://www.tithink.com/publicacion/MAGERIT.pdf>

Universidad Nacional de Colombia. (2018). Guía técnica colombiana ISO- 19011:2018. <http://siga.unal.edu.co/images/Modulos/Ova/Capacitacion_Guia_tecnica_auditoria_NTC_ISO_19011_2018.pdf>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Hernando José Peña Hidalgo | Experto Temático | Centro de la Industria, la Empresa y los Servicios - Norte de Santander | 12/Nov/2022 |
| Javier Ricardo Luna Pineda | Diseñador Instruccional | Centro De La Industria, La Empresa Y Los Servicios | Diciembre de 2022 |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| Autor (es) | Juan Guillermo Zuluaga Saavedra | Experto Temático | Regional Tolima – Centro de Comercio y Servicios | Septiembre 2023 | Revisión y actualización. |
| Humberto Arias Díaz | Diseñador Instruccional | Regional Tolima – Centro de Comercio y Servicios | Septiembre 2023 | Revisión y actualización. |
| María Inés Machado López | Revisora metodológica | Regional Tolima.  Centro de Servicios y Comercio | Noviembre de 2023 | Revisión de cambios 2023, revisión metodológica. |