**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Seguridad de aplicaciones web |
| --- | --- |

| COMPETENCIA | 220501108. Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501108-02 Evaluar los riesgos de seguridad digital para aplicaciones web acorde con los métodos definidos. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 02 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Fundamentos y aplicaciones de riesgo de seguridad orientada a aplicaciones web |
| BREVE DESCRIPCIÓN | La seguridad en aplicaciones web es una línea dentro de la seguridad informática que se delega concretamente sobre la seguridad de sitios web, aplicaciones web y servicios web |
| PALABRAS CLAVE | API, ciberseguridad, *hacking*, seguridad de la información |

| ÁREA OCUPACIONAL | 6 - Ventas y servicios |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

Introducción

* + - 1. **Introducción a la ciberseguridad**
      2. **Identificación de riesgos**
  1. Análisis de riesgos
  2. Herramientas de valoración de riesgos

1. **Auditoría infraestructura tecnológica**
2. **Informe o políticas de sistema de gestión de seguridad de la información o afines**
3. **Organización y protocolos de seguridad y privacidad**

**Síntesis**

1. **DESARROLLO DE CONTENIDOS**

**Introducción**

Le damos la bienvenida al componente formativo denominado “**Fundamentos y aplicaciones de riesgo de seguridad orientada a aplicaciones web”**, el cual hace parte del programa de formación técnico “Seguridad en aplicaciones web”, para lo cual se invita a observar el siguiente video:



* + - 1. **Introducción a la ciberseguridad**

La ciberseguridad, también conocida como seguridad informática o seguridad digital, es el área relacionada con la informática y telemática en la protección de la infraestructura computacional, ya sea una máquina o el parque computacional de una organización

La ciberseguridad se emplea en todo tipo de empresas públicas y privadas siendo aplicada en proyectos como: *home office* o teletrabajo, videoconferencias; cuando se habla de ciberseguridad abarca muchas líneas o áreas una de ellas es la seguridad en aplicaciones web y parte de las generalidades que en Colombia están enmarcadas en el Conpes 3701 de 2011 desarrollado por los Ministerios de Interior y de Justicia, Relaciones Exteriores, Defensa Nacional, Tecnologías de la Información y las Comunicaciones, Departamento Administrativo de Seguridad, Departamento Nacional de Planeación-DJSG-DIFP-DIES-OI, Fiscalía General, y que busca impulsar lineamientos de política en ciberseguridady ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente; por lo que se crea el grupo de respuesta a emergencias cibernéticas de Colombia colCERT*.*





Dentro de las figuras de ciberseguridad de una organización se encuentra al gerente o CEO, el departamento de Tecnología e Información (TI), el personal de seguridad informática o de la información y el departamento legal o jurídico, todos ellos desempeñan un rol importante en la actuación frente a un caso de un incidente informático o la protección de datos.

| La seguridad en aplicaciones web se considera como una rama de la ciberseguridad donde la misma busca preservar la integridad, confidencialidad y disponibilidad de la información.  Hoy en día, las empresas que están a la vanguardia de la transformación digital y en plena cuarta Revolución Industrial deben blindarse y proteger sus aplicaciones web, pero sobre todo el activo más importante dentro de una organización: la información que ingresa día a día y se puede verse afectada por diversas técnicas de *hacking* y los ataques informáticos que en Colombia y el mundo van en gran aumento. |  |
| --- | --- |

Es importante tener en cuenta que dentro de la ciberseguridad los principios de seguridad son la confidencialidad, integridad y disponibilidad

* La confidencialidad previene la divulgación de datos personales delicados cumpliendo con la normatividad legal del habeas data.
* La integridad garantiza la seguridad del contenido.
* La disponibilidad mantiene los datos siempre disponibles para los usuarios autorizados en la organización.

Con lo anterior, se puede afirmar que la ciberseguridad son las técnicas de procedimiento y uso de herramientas que se implementan con el único objetivo de proteger y blindar la información que se genera en computadores, dispositivos móviles, herramientas API, servidores, redes, información en la nube y sistemas electrónicos. Si una organización cuenta con personal capacitado en el área de la ciberseguridad y herramientas, sabrá detectar a tiempo los riesgos informáticos y afrontar con facilidad una vulnerabilidad o ataque informático.

* + - 1. **identificación de riesgos**

Se invita a ampliar el conocimiento sobre los riesgos informáticos, a través del siguiente video:



Dentro de los métodos de identificación de riesgos, la organización debe clasificar los tipos de riesgos en altos, medios y bajos; en este caso, en las aplicaciones web se revisan varios factores como, el lenguaje de programación y la arquitectura del software para poder empezar a analizar y trabajar sobre las posibles amenazas o vulnerabilidades.



 En el siguiente recurso se podrán conocer las técnicas de *hacking* utilizadas por los ciberdelincuentes:



La prevención de los riesgos se origina del análisis de las amenazas y vulnerabilidades que se detectan en la organización. La norma ISO 27005 contiene recomendaciones y normas que se deben llevar a cabo o tener en cuenta en los proyectos de aplicaciones web y que sirve de control ante futuras amenazas o riesgos informáticos.



El comercio electrónico que en Colombia está reglamentado a través de la Ley 527 de 1999 ha sido uno de los factores que ha llevado a las empresas a tener un crecimiento económico, pues dentro de la transformación digital una de las líneas de medición es la venta por medio de canales digitales o aplicaciones web.

Pero también existen diferentes factores de ataques en los que está la suplantación que es muy común en este tipo de aplicaciones web donde un pirata informático podrá alterar el contenido de una *cookie* y redireccionarlo a un servidor diferente.

* **Metodología o estándar para identificar riesgos en aplicaciones web**

Una metodología para identificar riesgos en aplicaciones web, podría ser a través de una matriz de riesgo de seguridad de la información, esta herramienta permite analizar o dar valor a los riesgos.

La matriz de riesgos 3 X 3 permite clasificar y valorar las diferentes vulnerabilidades comunes según la metodología OWASP dentro de las aplicaciones de sitios web de la siguiente manera:



Con la metodología *Open Web Application Security Project* (OWASP) se pueden aplicar técnicas de evaluación, tipos de controles frente a los riesgos, aplicar métodos de medición de controles y localizar vulnerabilidades.



Las diferentes acciones que se tomen ayudarían a jerarquizar el impacto, es importante que las aplicaciones en sitios web se corran en dominios aptos y seguros para la protección de la información de los usuarios.

* **Modelo OSI en la capa 7**

El modelo OSI en la capa 7 nivel de aplicación, presenta los siguientes protocolos:



* 1. **Análisis de riesgos**

En la identificación de riesgos se debe tener presente que:



Dentro de la gestión del riesgo de seguridad de la información se debe proteger la empresa ante las posibles consecuencias como pérdidas de confidencialidad, integridad, disponibilidad… también se tienen otras como no-repudio, autenticidad, o confiabilidad de los activos, el incumplimiento de la legislación, pérdidas financieras, impacto de orden público, impactos de orden internacional.

A continuación, se invita a conocer el ciclo PHVA, según la *Guía de gestión de riesgos de seguridad de la información*, presentada por el Icontec:



En las políticas lo primero será determinar el tratamiento que se le dará a cada uno de los riesgos identificados en la aplicación, donde se puede tomar la decisión de aceptarlos, transferirlos o ejercer controles apropiados según el nivel de riesgo. Posteriormente, habrá que determinar qué controles se pueden ejercer, una vez determinada la causa que los origina.

De acuerdo con lo anterior, los controles pueden ser de tipo:



Los anteriores controles buscan mitigar los riesgos de mayor impacto y la posibilidad de ocurrencia. Luego, se buscará integrar estos controles a las políticas y procedimientos empresariales para configurar un sistema de control denominado **sistema de gestión de seguridad de la información.**

**2.2 Herramientas de valoración de riesgos**

La valoración del riesgo asegura que para que el sistema logre los efectos previstos, con las mismas herramientas, se pueden prevenir o reducir efectos indeseados, logrando la mejora progresiva, integrando e implementando acciones en sus procesos.

Se puede encontrar también empresas en el mundo que ofrecen una gran cantidad de herramientas para la valoración del riesgo como:

* SpiraPlan de Inflectra Corp.
* Rastreados a 1.
* IsoMetriz y otras



1. **Auditoría infraestructura tecnológica**

Las auditorías informáticas internas o externas siempre son recomendadas para prevenir pérdidas o fugas de información y económicas en todos los aspectos (sanciones, ventas, ingresos, clientes, entre otros) para la organización; por ello, en cualquier infraestructura tecnológica estas auditorías se deben realizar al *hardware* por los requerimientos técnicos de la aplicación, en este caso, y el *software* para el análisis de vulnerabilidades o actualizaciones a los componentes de este garantizando la seguridad y confianza en las aplicaciones web.

Se deben tener en cuenta los aspectos técnicos de la aplicación, sin embargo se han elegido cuatro tipos de auditorías en aplicaciones web, a saber:



Dentro de los métodos de administración más complejos están las auditorías forenses, ya que estas tienen el objetivo de recolectar toda la evidencia digital y pruebas que permitan comprobar si existen o no fraudes, o delitos en una empresa, conforme a los protocolos nacionales e internacionales para mantener la integridad de la misma y su posterior cadena de custodia de la información; desde el punto normativo en Colombia se deben cumplir con los requisitos de los artículos 5°, 6° y 7° de la Ley 527 de 1999.



Dentro de la distribución de dominios en la auditoría informática está la planeación y organización donde es establece el cronograma y las diferentes estrategias de análisis o métodos para usar en la misma, seguidamente está la adquisición e implementación como establecer los diferentes correctivos y dar soluciones a los inconvenientes encontrados en la misma, además, se recomienda el servicio y soporte frente a los controles de aplicación sin dejar a un lado el monitoreo con el que toda organización debe evaluar frecuentemente la calidad, integridad y confidencialidad.

En cada auditoría se deben cumplir con los protocolos de seguridad informática, ya que hay que ceñirse a las reglas o normas donde se garantiza la confidencialidad, integridad y disponibilidad de toda la información.

1. **Informe o políticas de sistema de gestión de seguridad de la información o afines**

En la gestión de información, cuando se generan informes o documentos sobre los hallazgos y vulnerabilidades detectadas, estos deben contener un completo diligenciamiento con la compilación de datos recolectados por el técnico en seguridad de aplicaciones web.

El informe de auditoría sirve para verificar los cumplimientos de planes, estrategias y programas, los informes son necesarios para el monitoreo y toma de decisiones; este debe contener los siguientes ítems como resultados:



**5.** O**rganización y protocolos de seguridad y privacidad**

Gracias a internet el mundo vive interconectado; así, el protocolo TCP/IP se encarga de que cada ordenador, dispositivo móvil y servicio web disponible a través de internet cuente con una dirección IP exclusiva como 92.183.215.3. Así, el sistema DNS “indica”, con ayuda del servidor de nombres, esta dirección en un dominio como, por ejemplo, www.example.org, que al ojo humano le resulta más sencillo de leer. Este proceso también se denomina resolución de nombres.

A continuación, se podrán conocer algunos de estos protocolos de seguridad y privacidad:

**Tabla 1**

*Dominios*

| Protocolo | subdominio | nombre del dominio | extensión | descripción |
| --- | --- | --- | --- | --- |
| [https://](about:blank) | www | example | org | organización sin ánimo de lucro. |
| [https://](about:blank) | www | example | co | dirección de dominio Colombia. |
| [https://](about:blank) | www | example | blog | dirección de blog. |
| [https://](about:blank) | example | co | uk | dominio de tercer o cuarto nivel. |
| [https://](about:blank) | en | example | org | dirección para proyecto web. |

Así como la tabla de los dominios, se deben tener en cuenta los protocolos de aplicaciones oficiales de internet que se pueden usar.

* Domain Name Protocol (Protocolo de nombres de dominio).
* Exterior Gateway Protocol (Protocolo de pasarela exterior).
* File Transfer Protocol (Protocolo de transferencia de archivos).
* Name/Finger Protocol (Protocolo de nombres/finger).
* Telnet Protocol (Protocolo Telnet).

1. **SÍNTESIS**

En el siguiente recurso se podrá evidenciar un resumen de este componente formativo:

 

1. **ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Conceptos generales |
| Objetivo de la actividad | Identifique dentro de la actividad los conceptos de auditoría y de políticas de seguridad de la información. |
| Tipo de actividad sugerida | Ordenar numéricamente |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo5\_ActividadDidactica\_ CF02 |

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 |
| --- | --- | --- | --- |
| 2.1 Análisis de riesgos | Gestión del riesgo en la seguridad informática. (2005). *Amenazas y vulnerabilidades.* <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/> | artículo | https://acortar.link/DxVxwr |
| 2. identificación de riesgos | Icontec. (2013). ISO 2700*.* Icontec. | Página Web | https://www.icontec.org/ |
| 2. identificación de riesgos | National Institute Of Standars and Technology. (2002). *Metodología NSIT SP 800-30.* NSIT. | Articulo | [Metodologia-PSI-NUEVAProyecto.pdf (sld.cu)](https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf) |
| 3.Auditoría infraestructura tecnológica | Congreso de Colombia. (1999). Ley 527 de 1999. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> | Página Web | <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> |
| 3. Auditoría infraestructura tecnológica | Congreso de Colombia. (2009). Ley 1273 de 2009. <https://acortar.link/rY3Hyl> | Página Web | https://acortar.link/rY3Hyl |
| 3. Auditoría infraestructura tecnológica | Congreso de Colombia. (2012). Ley 1581 de 2012. <https://acortar.link/DB9gGZ> | Página Web | https://acortar.link/DB9gGZ |
| 4. Informe o políticas de sistema de gestión de seguridad de la información o afines | DNP. (2011). Conpes 3701 de 2011. <https://acortar.link/vVJlX8> | Página Web | <https://acortar.link/vVJlX8> |
| 4.Informe o políticas de sistema de gestión de seguridad de la información o afines | DNP. (2016). Conpes 3854 de 2016. <https://acortar.link/gtUi1u> | Página Web | https://acortar.link/gtUi1u |
| 4.Informe o políticas de sistema de gestión de seguridad de la información o afines | OAS. (2001). Convenio de Budapest. <https://acortar.link/lqGOIH> | Página Web | <https://acortar.link/lqGOIH> |

1. **GLOSARIO:**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Autenticación | acto de establecimiento o confirmación de algo como auténtico. La autenticación de un objeto puede significar la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores (educalingo, s. f.). |
| Base de datos | recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. Normalmente una base de datos está controlada por un sistema de gestión de base de datos (DBMS). En un conjunto, los datos y el DBMS, junto con las aplicaciones asociadas a ellos, reciben el nombre de sistema de base de datos, abreviado normalmente a simplemente base de datos (Oracle, 2022). |
| Evidencia digital | también conocida como evidencia computacional, única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados sino simplemente almacenados por o en computadores o medios equivalentes y registros o archivos híbridos que incluyen tanto registros generados por computador o medio equivalente como almacenados en los mismos (FGN, 2009). |
| *Log* | registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática un Log es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (*who, what, when, where* y *why, W5*) un evento ocurre para un dispositivo en particular o aplicación. La mayoría de los logs son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma cada log generado por un dispositivo en particular puede ser leído y desplegado en otro diferente. A su vez la palabra *log* se relaciona con el término evidencia digital. Un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales, lo que implica la lectura del *log* y deja al descubierto la actividad registrada en el mismo (FGN, 2009). |
| Redes | una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos (computadoras y/o dispositivos) conectados, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc. (FGN, 2009). |
| Seguridad informática | cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software (Gómez, 2006). Por su parte, Kissel (2012) la define como la protección de información y sistemas de información de acceso no autorizado. |
| Sistema de información | conjunto de procesos que, operando sobre una colección de datos estructurada de acuerdo con una empresa o entidad, recopila, elabora y distribuye (parte de) la información necesaria para el buen funcionamiento de ella. Además, apoya actividades de dirección y control correspondientes, apoyando al menos en parte, la toma de decisiones necesarias de acuerdo con su estrategia (FGN, 2009). |
| Transmisión de datos | movimiento de información codificada de un punto a otro(s) punto(s). Estos datos se transmitirán mediante señales eléctricas, ópticas, radio o electromagnéticas (FGN, 2009). |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Congreso de Colombia. (1999). Ley 0257 de 1999*.* Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html>

Congreso de Colombia. (2009). 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". <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

Congreso de Colombia, C. (2012)*.* Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf>

DNP. (2011). Conpes 3701. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

DNP. (2016). Conpes 3854. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Educalingo. (s.f.). *educalingo*. Obtenido de <https://educalingo.com/es/dic-es/autenticacion>

Erb, M. (2005). *Gestión de riesgo en la seguridad informática.* <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/>

FGN. (2009). *Procedimientos forenses de policía judicial.* FGN.

Gómez, A. (2006). *Enciclopedia de la seguridad informática.* RA-Ma .

Icontec. (2013). Icontec.<https://www.icontec.org/>

Mifsud, E. (2012). *Introducción a la seguridad informática.* <http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica>

National Institute of Standars and Technology. (2002). *Metodología PSI*. NIST. <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf>

OAS. (2001). OAS. <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf>

Oracle. (2022). Oracle. <https://www.oracle.com/co/database/what-is-database/>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Cesar Antonio Villamizar Núñez | Experto temático | Región Norte de Santander - Centro de la industria, la empresa y los servicios | Mayo de 2022 |
| Hernando José Peña Hidalgo | Experto temático | Regional Cauca, Centro de teleinformática y producción industrial | Mayo de 2022 |
| Carlos Hernán Muñoz | Experto temático | Regional Cauca, Centro de tele informática y Producción Industrial | Mayo de 2022 |
| Danny Alejandro Solano | Experto temático | Regional Cauca, Centro de tele informática y Producción Industrial | Mayo de 2022 |
| David Eduardo Lozada | Experto temático | Regional Cauca, Centro de tele informática y Producción Industrial | Mayo de 2022 |
| Paula Andrea Taborda Ortiz | Diseñadora Instruccional | Regional Norte de Santander, Centro de la Industria, la Empresa y Los Servicios CIES | Mayo de 2022 |
| Carolina Coca Salazar | Asesora Metodológica | Regional Distrito Capital- Centro de Diseño y Metrología | Junio de 2022 |
| José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital- Centro de Diseño y Metrología. | Julio del 2022. |

1. **CONTROL DE CAMBIOS**

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