

Incidentes y vulnerabilidades en seguridad orientada a aplicaciones web

**Breve descripción:**

Día a día las estadísticas por incidentes informáticos en el mundo aumentan, las diferentes técnicas de los ciberdelincuentes mejoran perfeccionando los ataques y cumpliendo con los objetivos que se proponen.

**Octubre 2023**

Tabla de contenido

[Introducción 1](#_Toc138636413)

[1. Título de nivel 1 **Error! Bookmark not defined.**](#_Toc138636414)

[1.1. Título de nivel 2 **Error! Bookmark not defined.**](#_Toc138636415)

[Título de nivel 3 **Error! Bookmark not defined.**](#_Toc138636416)

[2. Listas **Error! Bookmark not defined.**](#_Toc138636417)

[2.1. Listas ordenadas **Error! Bookmark not defined.**](#_Toc138636418)

[2.2. Listas no ordenadas **Error! Bookmark not defined.**](#_Toc138636419)

[2.3. Listas multinivel **Error! Bookmark not defined.**](#_Toc138636420)

[3. Extranjerismos **Error! Bookmark not defined.**](#_Toc138636421)

[4. Tablas **Error! Bookmark not defined.**](#_Toc138636422)

[4.1. Título de la tabla **Error! Bookmark not defined.**](#_Toc138636423)

[4.2. Fila o columna de encabezados **Error! Bookmark not defined.**](#_Toc138636424)

[4.3. Estilo de las tablas **Error! Bookmark not defined.**](#_Toc138636425)

[5. Imágenes **Error! Bookmark not defined.**](#_Toc138636426)

[5.1. Imágenes decorativas **Error! Bookmark not defined.**](#_Toc138636427)

[5.2. Imágenes informativas **Error! Bookmark not defined.**](#_Toc138636428)

[6. Video **Error! Bookmark not defined.**](#_Toc138636429)

[6.1. Título de video **Error! Bookmark not defined.**](#_Toc138636430)

[6.2. Portada del video **Error! Bookmark not defined.**](#_Toc138636431)

[6.3. Enlace y síntesis del video **Error! Bookmark not defined.**](#_Toc138636432)

[Síntesis 21](#_Toc138636433)

[Material complementario 22](#_Toc138636434)

[Glosario 23](#_Toc138636435)

[Referencias bibliográficas 26](#_Toc138636436)

[Créditos 28](#_Toc138636437)

Introducción

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

1. Incidentes y vulnerabilidades en seguridad orientada a aplicaciones web.



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=nmWZ75V7KHk)

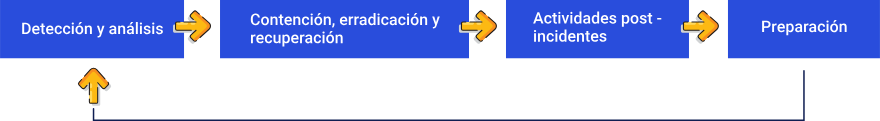
|  |
| --- |
| **Síntesis del video: Incidentes y vulnerabilidades en seguridad orientada a aplicaciones web.** |
| Incidentes y vulnerabilidades en seguridad orientada a aplicaciones web. Hola a todos, seguimos en la técnica de seguridad de la aplicación en web. En esta temática, vamos a hablar de una rama muy interesante que siempre se denomina como la "ciencia del futuro" cuando hablamos de informática forense. Vamos a hablar de incidentes informáticos, de la recopilación de esos incidentes informáticos y cómo redactar esos informes.  Frente a la sustentación de informática forense en Colombia, nuestro marco legal se rige bajo unos parámetros de cadena de custodia. Debemos recordar que la informática forense es frágil y volátil; es decir, la evidencia digital está compuesta por ceros y unos. Ustedes bien lo saben, pero hay unos parámetros o unos protocolos que se deben seguir, y estos protocolos son fundamentales. Estos procedimientos internacionales son realizados por grandes organizaciones como la Organización Internacional de Ciencia Computacional, así como los departamentos de inteligencia del FBI, de la CIA y de la DEA, que se han implantado en todo el mundo y en Colombia, por parte de nuestro procedimiento de la policía judicial.  La informática forense se encarga de mirar esos incidentes informáticos que ocurren en empresas, aplicaciones, páginas web o sistemas de información. Empezamos a hacer un análisis para determinar qué ocurrió, cómo ocurrió, dónde ocurrió y cómo fue toda esa ruta que la empresa va a establecer. Esto es importante manejarlo adecuadamente, porque por un mal procedimiento podríamos poner en duda toda esa evidencia digital y no se podría establecer una cadena de custodia adecuada, como lo rige el formato de cadena de custodia y el protocolo del mismo. Muchas gracias. |

# Incidentes informáticos

Dentro del tratamiento de incidentes de seguridad digital en las aplicaciones web, parte de la normatividad la establece el Ministerio de Tecnologías de Información y las Comunicaciones de Colombia mediante la Resolución 500 del año 2021 Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital”; por ello se debe recordar que al existir incidentes informáticos el Código Penal establece sanciones legales mediante la Ley 1273 de 2009.

Igualmente, hay que tener en cuenta los marcos de referencia ante un incidente de seguridad de la información guiándose con la ISO 27035 que es la norma de gestión de incidentes de seguridad de la información, el ciclo de vida de la gestión y contradicción de un incidente informático, así:

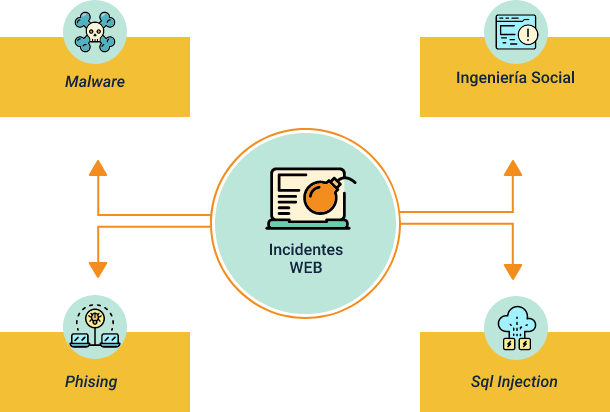
1. Ciclos incidentes informáticos



El ciclo siempre será repetitivo, el mismo puede controlarse o auditarse mediante políticas de seguridad de la información y que la organización tenga un departamento en atención frente a los diferentes incidentes de seguridad como un CSIRT como lo indica el Conpes 3701 de 2011; es necesario recordar que dentro los pilares de la información están:

* Confidencialidad.
* Integridad.
* Disponibilidad.

Los incidentes informáticos de seguridad en aplicaciones web pueden darse mediante técnicas de ingeniera social o “hacking” no autorizados, “malware” y SQL “injection”, como puede verse a continuación:



Se invita a conocer algunos conceptos importantes que identificará en el transcurso de este componente:

* **“Malware”.** Programas maliciosos que realizan acciones dañinas en un sistema informático.
* **Ingeniería social.** Técnicas usadas por organizaciones cibercriminales donde utilizan técnicas de engaño para que usuarios con desconocimiento o incautos envíen con facilidad datos confidenciales.
* **SQL “injection”.** Técnicas donde se usa código fuente realizando infiltraciones.

# Auditoría forense

Las auditorías forenses se realizan cuando los incidentes informáticos pasan a ser denunciados penal o administrativamente y se requieren para las investigaciones legales pertinentes, también se pueden realizar auditorías forenses para detener los incidentes informáticos y fortalecimiento de acciones dentro de la organización. En Colombia la ley con que más se enfrentan los ataques cibernéticos es la Ley 1273 de 2009 por la que se crea el bien jurídico tutelado y el dato.

Se recomienda que las auditorías forenses sean realizadas por externos y que tengan conocimiento en procedimientos de informática forense y derecho informático, esto debido que al recaudar evidencias digitales en un futuro las sustentará ante un estrado judicial.

Las etapas de la auditoría forense se conforman de la siguiente manera:

* Realización de auditoría forense.
* Definición de programas de auditoría forense.
* Ejecución de la auditoría forense.
* Elaboración del informe de auditoría forense.
* Entrega del informe al cliente.

## Informática forense

La informática forense es considerada la ciencia del futuro, la misma se realiza mediante la recopilación de log de auditoría del sistema o aplicación, o recuperar información borrada en los incidentes informáticos. En este proceso de incidentes se debe documentar y grabar los procedimientos e indicar los “software” forenses utilizados y procedimientos según los protocolos nacionales e internacionales.

El cómputo forense ayuda a detectar y analizar todas las pistas sobre ataques informáticos, conversaciones, robos de información o evidencia digital al navegar por internet, accesos no autorizados a aplicaciones y correos electrónicos. La finalidad es la de identificar, preservar, extraer y documentar para que estas evidencias digitales pasen a ser pruebas en un estrado judicial.

En Colombia, existe la unidad de delitos informáticos de la Fiscalía General de la Nación y el CAI virtual de la DIJIN unidad de incidentes informáticos. Cuando una aplicación web es vulnerada se debe identificar por medio de la Informática forense de dónde provino el ataque, cuál fue la técnica utilizada y revisar las posibles vulnerabilidades de la herramienta para tomar los correctivos de esta.

## Tableros de control

Los tableros de control se utilizan en las auditorías forenses para realizar chequeos y sacar conclusiones rápidamente, estos sirven para realizar tomas de información mediante los tableros de control; uno de ellos podría ser el siguiente:

Se invita a consultar el documento **Tablero de control análisis intermedio Auditoría forense** que se encuentra en la carpeta Anexos.

En los dominios se puede colocar el tipo del ciclo del PHVA, el tipo de proceso sería el de evaluar y administración de riesgos informáticos y dentro de cada objetivo de control son los contextos, identificación, evolución, evaluación o respuestas de los riesgos.

Como auditores, en cada ítem se realizan preguntas y se ejecuta como:

**Planear =** ¿Qué hacer? ¿Cómo hacerlo?

**Hacer =** Ejecutar lo proyectado.

**Verificar =** ¿Las cosas transitaron según cronograma planteado?

**Actuar =** ¿Cómo mejorar la próxima vez?

Al empezar a aplicar el ciclo PHVA, en la acción planear se debe conocer los procesos digitales críticos en la organización, luego detalladamente se analizan, para implementar controles que protejan los procesos implementados ante amenazas cibernéticas.

Un ejemplo de un objetivo de control sería: identificación de riesgos.

Dentro de la lista de chequeo se pueden realizar preguntas y reformular las mismas conforme a la organización, frente al manejo y operación de las aplicaciones web donde se marca solo un ítem entre sí o no y una observación general en caso de justificar, la misma del ítem seleccionado; de igual forma, se pueden agregar más aspectos a evaluar dependido el análisis o tipo de auditoría o control que requiere realizar el profesional. A continuación se presenta dicho formato:

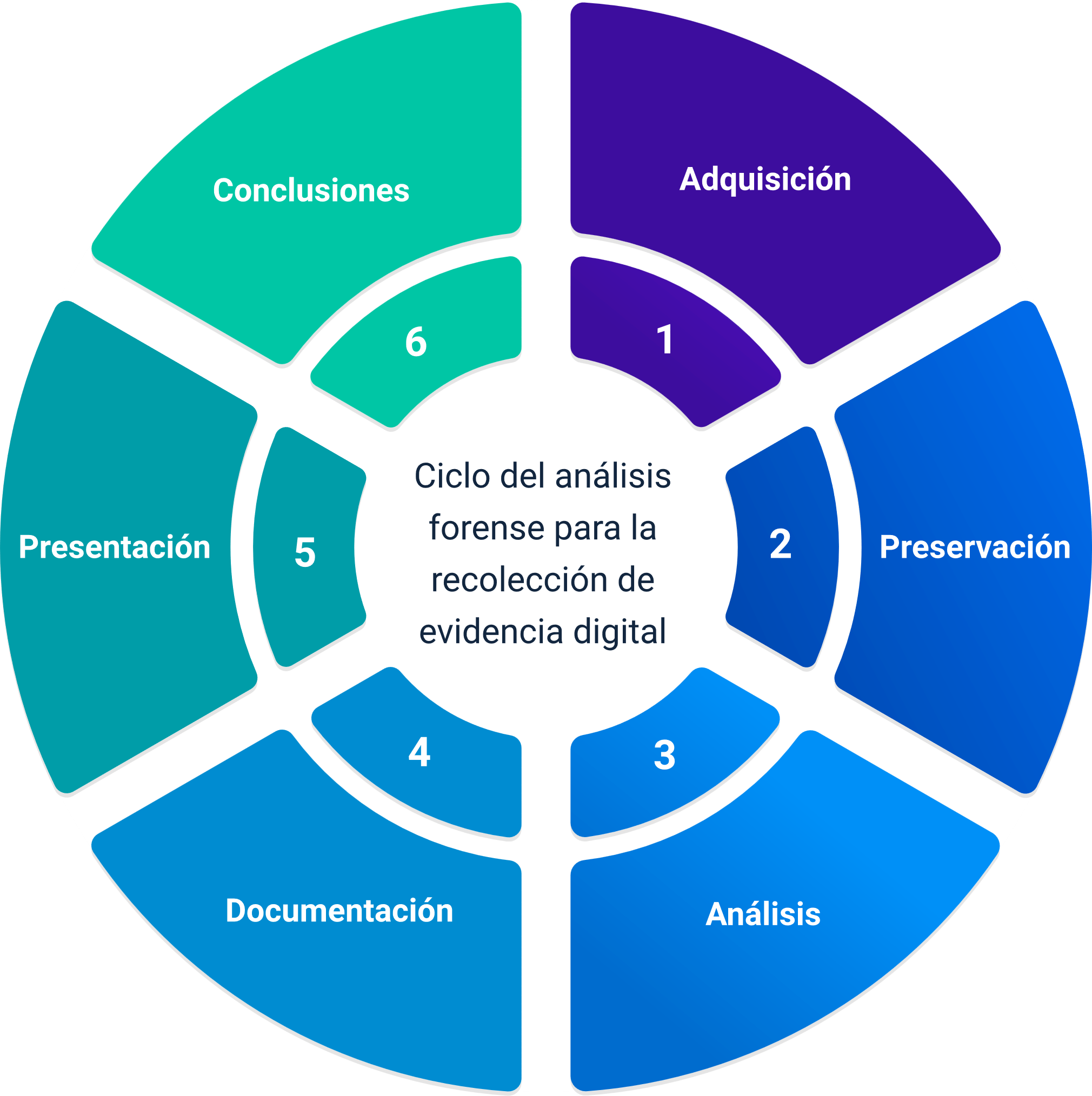
Se invita a consultar el documento anexo **Lista de chequeo control básico,** para ampliar sus conocimientos

# Recolección de evidencia digital

La IOCE (Organización Internacional de Evidencia Computacional) estableció en el año 1999 cinco principios internacionales para tener en cuenta para el adecuado manejo de la evidencia digital. Se invita a saber de qué tratan:

* **Principio 1.** Al recolectar la evidencia digital se deben tomar acciones para asegurarse de que no se modificará dicha evidencia.
* **Principio 2.** Cuando una persona necesite acceder a la evidencia digital original, se debe asegurar que sea un investigador forense competente.
* **Principio 3**. Toda la actividad relacionada con la recolección, acceso, almacenamiento o transferencia de evidencia digital debe estar documentada, preservada y disponible para ser revisada.
* **Principio 4.** Un individuo es responsable por todas las acciones realizadas sobre la evidencia digital mientras esta se encuentre en su posesión.
* **Principio 5.** Cualquier agencia que sea responsable de la recolección, acceso, almacenamiento o transferencia de evidencia digital es responsable de cumplir con los principios anteriores.

Además, toda evidencia digital es frágil y volátil, por lo que la misma se debe recolectar de manera adecuada para no ponerla en duda. A continuación, se relaciona el ciclo de la evidencia digital:



Cuando se habla de adquisición en el análisis forense, se hace con base en los parámetros del formato cadena de custodia quien halla, recolecta y embala la misma; la preservación nos indica la técnica con la herramienta de “software” forense utilizada para mantener la idoneidad de esta.

El análisis es aquel que se realiza en el laboratorio forense para realizar procedimientos en caso de borrado de navegación o al sistema de información, en la documentación debe ir explicado todo desde el inicio: características informáticas del “software”, método utilizado, identificación del perito informático, tamaño de la información, nombre y versiones del “software” forense usado. La presentación es la terminación de ese informe junto con la evidencia digital recolectada cumpliendo los procedimientos forenses, y las conclusiones son con base en lo analizado y lo que no se pudo recuperar.

# Informes incidentes de seguridad en aplicaciones

Antes de iniciar este tema, es importante observar el siguiente video explicativo:

1. Informes preliminares.

A close-up of a keyboard

Description automatically generated

[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=Fnu6k-qrlGg)

|  |
| --- |
| **Síntesis del video: Informes preliminares** |
| Informes preliminares: Hola, dentro de los informes de informática forense, deben ser unos informes muy completos que se deben regir por unos parámetros o por unos protocolos internacionales y nacionales. Es decir, la IOC (Organización Internacional de Evidencia Computacional) establece cinco principios frente a eso. La evidencia debe ser analizada por personas expertas y capacitadas en el área. Además, esa evidencia no puede cambiar por ningún motivo. Las agencias o personas que se encargan de recolectar esa información o esas evidencias digitales deben ser documentadas. Las mismas deben ser preservadas y manejadas adecuadamente, y esto no se puede poner en duda al sustentar los informes forenses en el futuro.  Todo informe forense debe llevar un procedimiento de inicio y un procedimiento paso a paso, como la recolección. ¿Qué herramientas utilizó para la recolección? Si utilizó herramientas gratuitas o herramientas pagas, debemos recordar que las herramientas pagas son herramientas que solamente cuentan las organizaciones internacionales y los organismos de inteligencia de cualquier país. Esto se debe a que estas aplicaciones son costosas y que cada cuatro o seis meses se van actualizando y su valor va incrementando.  Por eso, es importante que cuando se hagan esos informes preliminares, como por ejemplo, dentro del parámetro de la cadena de custodia, al formato de cadena de custodia, está quien recolecta y quien embala. En este caso, ustedes serán los primeros que lleguen allí frente a un incidente informático. Todo debe estar muy bien documentado desde el punto de vista científico y profesional en su área. Con su conocimiento, podrá decir: Esto ocurrió tal día, a tal fecha, en tal momento se realizó este procedimiento. Ese procedimiento fue grabado mientras que yo lo iba revisando. Extraímos un blog, miramos el tema de auditoría, revisamos cámaras, frente al mismo, en caso de que fueran en el lugar, revisamos trazabilidad de redes, miramos ubicación, parametrización y una gran cantidad de componentes. Dependiendo del escenario o del tipo de ataque, cada escenario y cada tipo de ataque tiene un procedimiento diferente.  Por eso, es importante regirnos frente al tema forense, pero no dejar de un lado el tema legal. La Ley 527 del 99 establece unos principios frente a los mensajes de datos. Es decir, el artículo 5, 6 y 7 hablan de escrito, firma y originalidad. Cuando el mensaje de datos lleva una firma, ¿qué procedimiento matemático o científico utilizó usted para no poner en duda esa información? Y puede ser analizada por otros peritos forenses. La originalidad que se mantenga frente a la información, es decir, la metadata, recordemos que todos los archivos, sea el que sea (un archivo Word, Excel, PowerPoint, una página, una aplicación), tienen unos metadatos internos como la fecha de creación, fecha de modificación, fechas de últimos registros, registro de entrada, horario, el tipo de software, la versión, etcétera, que se puede manejar en el mismo. Nosotros debemos empezar a mirar frente a esto qué se puede obtener o se debe aplicar para que realmente no se pongan dudas sobre la integridad, la confidencialidad y la originalidad de la información. Muchas gracias para todos. |

Los informes se deben presentar claros, concisos y ordenados, los mismos deben ser exhaustivos respecto de las técnicas forenses utilizadas con conclusiones lógicas, bien argumentadas y en un lenguaje técnico, legal y explicativo para los demás.

Lo anterior mediante el ASVS, que es un marco de referencia de requisitos de seguridad, controles funcionales y los no funcionales que se requieren al diseñar, desplegar y testear aplicaciones web. Así como con el OWASP top 10 que es el documento principal para tener en cuenta sobre los riesgos de seguridad más destacados en aplicaciones web, como se indica en la tabla a continuación:

1. Metodología de clasificación de riesgo

| Agente de amenaza | Explotabilidad | Prevalencia de vulnerabilidad | Detección de vulnerabilidad | Impacto técnico | Impacto de negocio |
| --- | --- | --- | --- | --- | --- |
| Específico de la aplicación. | 3 Fácil. | 3 Difundido. | 3 Fácil. | 3 Severo. | Específico del negocio. |
| Específico de la aplicación. | 2 Promedio. | 2 Común. | 2 Promedio. | 2 Moderado. | Específico del negocio. |
| Específico de la aplicación. | 1 Difícil. | 1 Poco común. | 1 Difícil. | 1 Mínimo. | Específico del negocio. |

**Factores de riesgo**

Para conocer los factores de riesgo que se asocian a la anterior tabla, le invitamos a descargar el documento **Factores de riesgo** que se encuentra en la carpeta Anexos.

Según las tablas anteriores y los niveles de riesgos detectados por cada ítem de análisis en el informe, se debe especificar el tipo de amenaza según la aplicación, así:

1. Impacto vs. valoración

|  |  |  |
| --- | --- | --- |
| Impacto | Descripción | Valoración |
| Catastrófico | Extremadamente dañino | Alto |
| Mayor | Dañino | Alto |
| Moderado | Moderado | Medio |
| Menor | Menor | Baja |
| Insignificante | Ligeramente dañino | Baja |

La descripción de la anterior tabla, se puede interpretar de la siguiente manera:

* **Impacto catastrófico y riesgo alto.** La descripción es extremadamente dañina, en la misma en el informe se pone el valor de pérdidas superiores a 1.500 SMLV, la afectación de la imagen corporativa a nivel local, regional, nacional e internacional. Si llega a tener sanciones por entes de control como Fiscalía, Procuraduría y Contraloría, y también analizar si hay graves daños en la infraestructura y aplicaciones web de la organización.
* **Impacto mayor y riesgo alto.** Sería una descripción de tipo dañino si existen pérdidas económicas entre 1.000 y 1.499 SMLV, si la afectación de la imagen corporativa es a nivel local, regional y nacional. Si llega a tener sanciones por entes de control como Fiscalía, Procuraduría y Contraloría y también analizar si hay graves daños en la infraestructura y aplicaciones web de la organización.
* **Impacto moderado y riesgo medio**. Sería una descripción de tipo moderado si existen pérdidas económicas entre 600 y 999 SMLV, si la afectación de la imagen corporativa es a nivel local. Si llega a tener sanciones a nivel de la oficina de control interno o jurídico de la entidad, y también analizar si hay daños parciales en la infraestructura y aplicaciones web de la organización.
* **Impacto es menor y el riesgo bajo.** Sería una descripción de tipo menor si existen pérdidas económicas entre 400 y 599 SMLV, si la afectación de la imagen corporativa es a nivel organizacional. Si llega a tener sanciones a nivel procesos, y también analizar si hay daños pequeños en la infraestructura y aplicaciones web de la organización.
* **Impacto es insignificante y el riesgo bajo.** Sería una descripción de tipo ligeramente dañino si existen pérdidas económicas menores a 399 SMLV, si la afectación de la imagen corporativa es a nivel de área, si llega a tener sanciones a nivel área, y también analizar si hay daños pequeños en la infraestructura y aplicaciones web de la organización. Hay que revisar si se tiene llamados de atención a nivel grupo.

En la organización, y en este caso con las aplicaciones web, pueden ocurrir varios impactos y diferentes valoraciones que deben ser documentados y analizados en el informe, y de igual manera establecer un plan de mejora y control frente a incidentes informáticos.

En cuanto a la urgencia frente a incidentes informáticos en aplicaciones web, se tienen de la siguiente manera:

#### Atención a la urgencia

* **Alto.** El incidente de seguridad debe atenderse entre 0 y 120 minutos.
* **Medio**. El incidente de seguridad debe atenderse entre 0 y 240 minutos.
* **Bajo.** El incidente de seguridad debe atenderse entre 0 y 1.440 minutos.

Estos tiempos de respuestas también deben de ser tenidos en cuenta en la realización del informe, tener en cuenta los tiempos mínimos y máximo según el incidente informático en la aplicación web. Es importante establecer políticas de control en las aplicaciones web; la ISO 27001 juega un papel fundamental en ese plan de mejora.

Un informe de auditoría debe contar con todas las evidencias recolectadas (logs, errores humanos detectados, irregularidades) y el procedimiento es el siguiente:

* Aplicar instrumentos de toma de información.
* Registrar las situaciones encontradas.
* Comentar las situaciones encontradas y sus posibles causas.
* Analizar y depurar las situaciones relevantes.
* Comentar las situaciones relevantes con gerente o directivos.
* Elaborar informe final con dictamen del auditor y plan de mejora.
* Sustentar informe final ante directivos o gerente.

En los informes de incidentes de seguridad en aplicaciones, se incluyen los ajustes de controles que hacen referencia a los planes de mejora; así se detienen y previenen futuros incidentes informáticos, ya que los mismos buscan establecer mecanismos de prevención y control. Como política general de ajuste de control se debe contemplar las actualizaciones de “software” o parches de seguridad en la herramienta de aplicaciones web cada vez que se detecte una. A continuación, se conocerá los niveles de planes de mejora y tablero de control, básico, intermedio y avanzado:

**Básico**

* Antivirus.
* Contraseñas fuertes.
* Realizar “backup” frecuentes.
* Actualizar “app”.

**Intermedio**

* No reciclar contraseñas.
* Usar gestor de contraseñas.
* Actualizar personal.
* Utilizar “firewall”.
* Proteger servidores web.

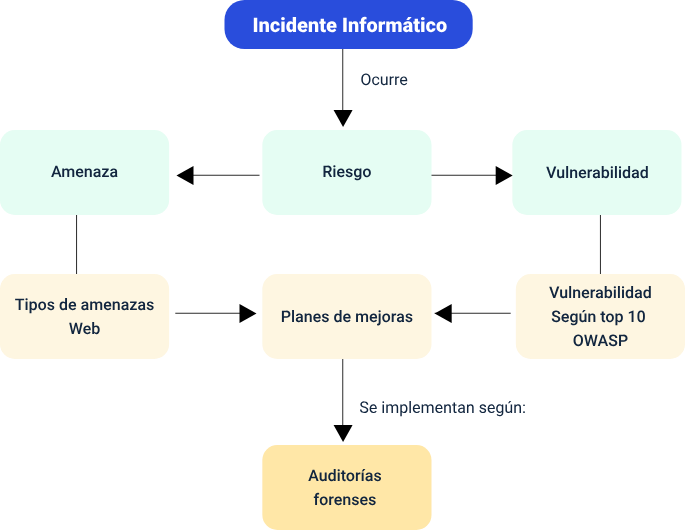
**Avanzado**

* Utilizar cifrado.
* Actualizar tableros de control de amenazas y riesgos.
* Tener configuraciones avanzadas de seguridad web.

Los planes de mejora son las conclusiones que toda auditoría deja por defecto tomando correctivos para que los riesgos y amenazas no vuelvan a la aplicación web, con este tipo de control y seguimiento se previenen riesgos y amenazas.

Síntesis

Ya se conoció en detalle las diferentes temáticas abordadas en este componente formativo, ahora es momento de verlas de manera resumida y puntual a través del siguiente esquema conceptual:



Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| 1. Incidentes informáticos | Incibe. (s. f.). Gestión de riegos. | Documento | <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf> |
| 3. Recolección de evidencia digital | Oficina de Seguridad para las Redes Informáticas. (s. f.). Metodología para la gestión de la seguridad informática (proyecto). | Articulo | <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf> |
| 3. Recolección de evidencia digital | Congreso de Colombia. (1999). Ley 527 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. | Ley | <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> |

Glosario

**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 desde el punto digital tenemos varios tipos de autenticación como las contraseñas, biométricos, “token” y otros. (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)

Referencias bibliográficas

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. (2012). Ley Estatutaria 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). Documento Conpes 3701. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

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

Educalingo. (s.f.). Autenticación. <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.

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

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

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

Créditos

| Nombre | Cargo | Centro de Formación y Regional |
| --- | --- | --- |
| Claudia Patricia Aristizabal | Responsable del Ecosistema | Dirección General |
| Rafael Neftalí Lizcano Reyes | Responsable de Línea de Producción | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Cesar Antonio Villamizar Núñez | Experto Temático | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Hernando José Peña Hidalgo | Experto Temático | Centro de Teleinformática y Producción Industrial - Regional Cauca |
| Carlos Hernán Muñoz | Experto Temático | Centro de Teleinformática y Producción Industrial - Regional Cauca |
| Danny Alejandro Solano | Experto Temático | Centro de Teleinformática y Producción Industrial - Regional Cauca |
| David Eduardo Lozada | Experto Temático | Centro de Teleinformática y Producción Industrial - Regional Cauca |
| Paula Andrea Taborda Ortiz | Diseñadora Instruccional | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Centro de Diseño y Metrología - Regional Distrito Capital |
| José Gabriel Ortiz Abella | Corrector de estilo | Centro de Diseño y Metrología - Regional Distrito Capital |
| Carmen Alicia Martínez Torres | Animador y Productor Multimedia | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Wilson Andrés Arenales Cáceres | Storyboard e ilustración | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Camilo Andrés Bolaño Rey | Locución | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Blanca Flor Tinoco Torres | Diseñador de Contenidos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Andrea Paola Botello De la Rosa | Desarrollador Fullstack | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Andrea Paola Botello De la Rosa | Actividad didáctica | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Daniel Ricardo Mutis Gómez | Evaluador para Contenidos Inclusivos y Accesibles | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Zuleidy María Ruíz Torres | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Luis Gabriel Urueta Álvarez | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |