

CIBERSEGURIDAD Y BIG DATA

AUTOR: JORGE MARIO OCHOA VÁSQUEZ





CONTENIDO

INTRODUCCIÓN	3
1. SEGURIDAD EN CAPAS.....	4
2. DETECCIÓN DE INCIDENTES	7
2.1. Sistemas SIEM como forma de abordar la ciberinteligencia.....	8
2.2. MISP como propuesta de plataforma para la ciberseguridad	9
3. CONTINUIDAD DEL NEGOCIO	11
4. PLAN DE RECUPERACIÓN ANTE DESASTRES (PRD).....	12
5. AUDITORÍA.....	14
5.1. Pasos de auditoría de la base de datos.....	15
6. BIG DATA EN EL ÁMBITO DE LA CIBERSEGURIDAD	18
BIBLIOGRAFÍA	20



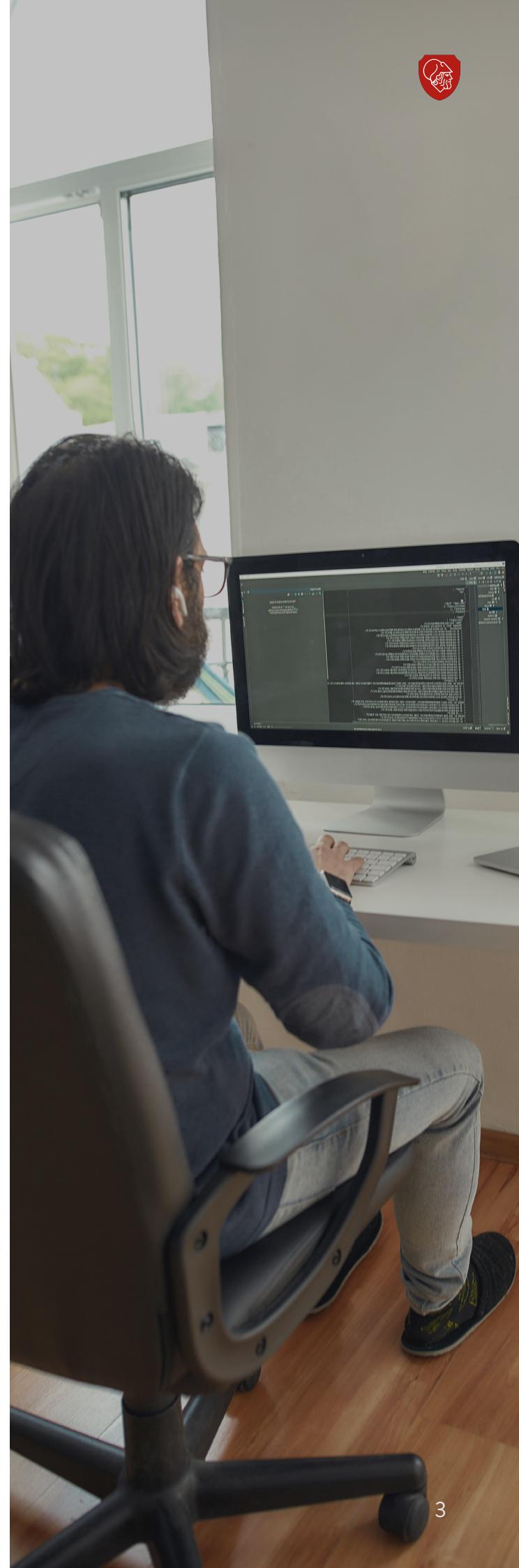


INTRODUCCIÓN

Tener en cuenta la seguridad al programar y desarrollar debe ser prioritario. Un sistema debe ser confiable, desarrollar un código seguro es prioritario para el correcto funcionamiento. Pero siempre hay que tener en cuenta que un sistema puede ser vulnerado, entonces hay que hacerlo con especial cuidado.

Tratar de mantener los sistemas simples ayuda a la hora de encontrar errores. La complejidad que un sistema posee de forma interna es directamente proporcional al tiempo que cuesta detectar, analizar y responder ante un incidente de seguridad. Por lo que encontrar errores o vulneraciones puede ser un trabajo intenso.

La ciberseguridad se aplica en todas las empresas, la información puede tener un valor incalculable. Aprender cómo resguardar datos y protegernos es de gran importancia, ya que también un buen sistema también puede generar buena confianza con clientes y personal que trabaje con nosotros generando mejor rendimiento.





01

SEGURIDAD EN CAPAS

Desarrollar un software robusto y seguro frente a amenazas va más allá de las líneas de código, sin menospreciarlo pues, aunque es muy ventajoso no es suficiente. Un sistema seguro requiere una arquitectura segura en conjunto e interrelaciones que tenga en cuenta la seguridad y la gestión de riesgos.

Los principios de seguridad son la base y la guía para proteger cualquier sistema en cualquier momento: tanto al modificar una línea de código como para la funcionalidad de una aplicación. Los documentos de diseño, desde el punto de vista de seguridad, sirven de guía para el resto de las fases con el fin de obtener un código seguro. A continuación, los diez principios claves del diseño seguro:

1. Seguir el principio de mínimo privilegio

Cada proceso solo debe tener la información y recursos necesarios para su función y no más, debe cumplir sólo la función necesaria y si tuviese otra se debe eliminar. En ejemplos sencillos de comprender, si un usuario solo se encarga de un departamento, este solo debe tener acceso a ese departamento y no a todos ellos; asimismo, si se requieren conservar todas las facturas emitidas, no se necesita y por consiguiente no debe existir un botón para eliminarlas.

2. Establecer seguridad por defecto:

Se debe procurar que sea lo más restrictivo posible. En caso de necesitar más permisos, estos deben establecerse después con una acción.

Es conveniente que el desarrollador deba especificar los métodos que son accesibles al público en vez de limitar las que no lo son. Partiendo del principio de que es más fácil detectar una puerta “cerrada” (pues el sistema requerirá que la “abras”) que una “abierta” y propensa a vulnerabilidad.



3. Implementar seguridad en profundidad

Un método de seguridad puede fallar, todo componente puede ser vulnerado así que no se puede confiar en un solo método por más seguro que sea ya que si es atacado, no se tendrá la capacidad ni tiempo de respuesta en caso de que sea superado.

En este caso se recomienda contar con varios sistemas de protección, imaginando las capas de una cebolla, donde cada una contiene un nivel de seguridad. De esta manera, si uno falla se tendrán otros métodos que impedirán el ataque al software y permitirá dar una mejor respuesta mientras los atacantes intentan vulnerar las capas sucesivas.



Figura 1. Ciberseguridad.
(Shutterstock, 2021).

4. Reducir la superficie de ataque

Todos aquellos puntos en los que un atacante (mediante prueba manual o automática) puede interactuar, introduciendo datos y/o extrayéndolos se le llaman vectores de ataque y son parte de la superficie de exposición o de ataque de una aplicación o sistema.



Figura 2. Programando
(Shutterstock, 2021).

Un principio básico de seguridad es eliminar o reducir todos estos puntos de la superficie de ataque que exponen al sistema, a la menor superficie posible, minimizando los riesgos.

5. Asegurar el eslabón más débil

La ley de la cadena: un equipo es tan fuerte como su eslabón más débil. En este sentido, los atacantes buscan el sistema (o el punto de este) que le sea más fácil, así el punto crítico de una aplicación o sistema es este punto más débil. Verificar y aumentar su seguridad es vital para hacer frente a las vulnerabilidades del sistema.

6. Validar los datos de entrada

Muchos ataques a sistemas informáticos se basan en introducir unos datos que el sistema no controla y no espera. Por tanto, todos los datos de entrada a la aplicación o sistema deben ser controlados en torno a su validación de tamaño y forma. Con el propósito de eliminar muchas posibilidades para el atacante, es preferible desconfiar de todos los datos ingresados asumiendo que cada entrada de cada dato puede ser maliciosa.





7. Seguir una separación de privilegios

La suplantación de identidad o el fraude de una persona con permiso total afectará completamente al sistema y las consecuencias serán muy graves. La recomendación es definir diferentes roles y permisos asociados a cada usuario, delegando la capacidad y responsabilidad de tomar acciones sobre el sistema.



Figura 3. Mantenimiento. (Shutterstock, 2021).

8. Mantener la simplicidad del sistema

En general, los sistemas funcionan mejor si se mantienen simples en vez de complejos, todo lo que no aporte un beneficio debe ser evitado. La complejidad que un sistema posee de forma interna es directamente proporcional al tiempo que cuesta detectar, analizar y responder ante un incidente de seguridad.

En otras palabras, entre más elementos extras tenga el sistema, el margen de error y de aparición de vulnerabilidades aumenta de manera innecesaria; entre más difícil de entender es uno de sus elementos, más posibilidades hay de que ocurra un incidente.

9. Implementar un correcto manejo de errores y excepciones

Una respuesta incorrecta o un mensaje de error desacertado puede exponer información interna a personal no autorizado y llamar la atención de un atacante, provocando un intento de ataque o incluso apoyando su preparación. En consecuencia, la aplicación debe ser diseñada y programada de tal manera que todas las excepciones y errores estén previstas con una respuesta planificada.

Estos errores en sí mismos también pueden provocar un incidente de seguridad, causando una parada del servicio que produzca una corrupción o pérdida de datos.

10. Implementar trazabilidad, registro de log y eventos de seguridad

Mantener un registro e implementar un sistema de notificación de problemas es importante para la seguridad. Es clave identificar y entender un ataque en proceso o ya terminado. Por ende, con el registro de log los eventos se pueden identificar en tiempo real durante la ejecución del software. Esta información permite mejorar el sistema y prepararse ante nuevas amenazas.



Figura 4. Nuevas configuraciones. (Shutterstock, 2021).



02

DETECCIÓN DE INCIDENTES

Cuando se analizan los eslabones débiles propensos a un riesgo alto se encuentra que muchos ataques comienzan con la ingeniería social, por ejemplo:

- **El phishing:** sucede cuando el atacante envía correos electrónicos de apariencia legítima en un intento de recopilar información personal y financiera de los destinatarios. En este sentido, generalmente los mensajes parecen provenir de sitios web conocidos y confiables o bien tener un tono de alarma asociado.
- **La inyección SQL:** aprovecha las vulnerabilidades de entrada no validadas para pasar comandos SQL a través de una aplicación web para su ejecución en backend.
- **La exfiltración de datos:** consiste en la copia, transferencia o recuperación no autorizada de datos de una computadora o servidor. También se conoce como extrusión de datos, exportación de datos o robo de datos.
- **El servidor de ensayo:** es un servidor que permite ensamblar, implementar y probar un software o un sitio web en una instancia de servidor, similar al servidor de producción.



IMPORTANTE

No hay un criterio unificado para abordar la ciber inteligencia. Hoy en día se cuenta con varios enfoques, tanto desde el ámbito de políticas estatales o desde organizaciones empresariales. El punto en común es el de homogeneizar la metodología de extracción de información.



2.1. SISTEMAS SIEM COMO FORMA DE ABORDAR LA CIBERINTELIGENCIA

El término se deriva de la combinación de dos tecnologías: SIM (Security Information Management) y SEM (Security Event Management). De allí surge SIEM (Security Information and Event Management) el cual se presenta como una responsabilidad interna de la organización o como un servicio ofrecido por un ente externo especializado en seguridad de la información.

Los SIEM tienen rápida velocidad de respuesta ante los incidentes hallados y son capaces de generar la detección de exfiltración de datos, detección de amenazas o de cualquier actividad sospechosa o poco usual.

La problemática surge si todos los logs generados por un SOC (Centro de Operaciones de seguridad) están deslocalizados, causando que los incidentes sean muy difíciles de detectar. Por medio de un SIEM se pueden centralizar todos esos logs y mediante diversos métodos de análisis de datos e inteligencia artificial se pueden gestionar eficientemente de modo que se apliquen las respectivas medidas que ayuden a detectar los posibles incidentes para contrarrestar los ataques o robos al sistema.

Los componentes y capacidades de los SIEM son los siguientes:



Figura 5. Diagrama de componentes y capacidades de los SIEM. (Elaboración propia, 2021)



- **Agregación de los datos:** Hacer un respaldo de los múltiples eventos de seguridad para conformar la base de las demás tareas del SIEM.
- **Correlación:** busca determinar patrones y detectar acciones irregulares mediante la vinculación que se determina en los eventos y datos.
- **Analítica:** identifica los indicadores más profundos que puedan ayudar a realizar actividades de seguridad avanzada usando machine learning o modelos matemáticos o estadísticos.
- **Uso de fuentes externas:** relaciona los datos internos de la organización con los proporcionados por organizaciones externas, el motivo es permitir la identificación de amenazas comunes u otros indicadores maliciosos.
- **Alertas:** Luego de analizar los eventos se busca una condición de disparo que repercuta en la debida respuesta o atención del incidente.
- **Dashboards:** presenta la información de la base de datos de forma visual a fin de facilitar la revisión.
- **Compliance:** Se trata de gestionar la automatización para el cumplimiento de las normas de seguridad de la empresa.
- **Retención:** comprende un respaldo de la base de datos a lo largo del tiempo, lo cual mantiene los datos por un tiempo prolongado para hacer el análisis y los estudios avanzados de los comportamientos, a su vez que cumple con las políticas de retención de logs.
- **Threat Hunting:** consiste en el análisis en base a consultas, filtros o pivoteo de los datos para descubrir amenazas o vulnerabilidades.
- **Incident Response:** se refiere a las acciones que se generan como consecuencia de un mensaje de alerta o como detección de algún incidente.
- **Automatización SOC:** implica automatizar las respuestas de las amenazas detectadas de forma eficiente, procurando la rapidez de la respuesta. Es la característica que distingue a los SIEM actuales.

2.2. MISP COMO PROPUESTA DE PLATAFORMA PARA LA CIBERSEGURIDAD

En 2012 un grupo de analistas de seguridad de distintos organismos se dieron cuenta que trabajaban en el mismo malware, como respuesta crean una plataforma colaborativa para unificar sus esfuerzos y ser más eficientes, como resultado aparece el MISP (Malware Information Sharing Platform) una plataforma de software libre (código abierto) sostenida ahora por un grupo de desarrolladores del CIRCL y muchos otros colaboradores.



IMPORTANTE

Las mejoras implementadas en los SIEM (Security Information and Event Management) se lo debemos al análisis avanzado de los logs mediante la inteligencia artificial que detecta amenazas desconocidas de un sistema. En este orden de ideas, es importante la retención de los logs ya que con la conjunción de la Big Data y la inteligencia artificial se podrían conocer elementos importantes para reforzar la seguridad.



MISP es una plataforma para compartir indicadores de amenazas, inteligencia de amenazas dentro de los sectores público y privado. Su función es recopilar, almacenar, distribuir y compartir indicadores de seguridad de forma estructurada y eficiente.

Sus principales objetivos son:

- Facilitar el almacenamiento de información sobre malware detectados.
- Relacionar el malware y sus propiedades por medio de rastros de intrusión y otros indicadores de correlación.
- Hace que la base de datos esté disponible automáticamente al guardar los datos en un formato estructurado.
- Generar reglas y propiciar normas para el sistema de detección de instrucciones en la red (NIDS) que se pueden importar en los sistemas IDS (Intrusion Detection System).
- Registrar y compartir los indicadores de amenazas con otras organizaciones a la vez que mejora la detección y reversión de malware.
- Facilitar el uso de plataformas confiables, garantizando la confidencialidad de las consultas pues almacena localmente toda la información de otras instancias.





03

CONTINUIDAD DEL NEGOCIO

Una parte vital de la gestión de seguridad de sistemas de información (SGSI) comprende el plan de continuidad del negocio, el cual dicta las pautas para sobrelevar los incidentes e infortunios en la empresa. El estándar internacional para la continuidad del negocio lo define la norma ISO 22301 como la “capacidad de continuar la prestación de productos o servicios en los niveles predefinidos aceptables tras incidentes de interrupción de la actividad”.

El proceso de lograr esta capacidad y mantenerla es tarea de la gestión de la continuidad del negocio (BCM, por sus siglas en inglés) y consta de seis etapas:

- **Etapa 1.** Creación del programa de BCM. Se realiza tomando en cuenta el tamaño y complejidad de la organización, delegando a los responsables y asignando sus tareas en la gestión de continuidad del negocio.
- **Etapa 2.** Comprensión de la compañía. Para ello se recolectan datos clave sobre los bienes involucrados en la realización de las funciones críticas, con el propósito de clasificar las actividades en clave, de apoyo y asignar los recursos. Incluye la evaluación del impacto del negocio y de los riesgos.
 - **Etapa 3.** Definición de estrategias: todo debe quedar documentado en los acuerdos vigentes: desde las medidas para la pronta recuperación hasta el caso extremo de mudar las operaciones temporalmente.
 - **Etapa 4.** Elaboración y ejecución de una respuesta: se documenta paso a paso cómo será el proceso de notificación para los miembros de la empresa y el proceso de asesoramiento de los clientes.
 - **Etapa 5.** Cumplir los acuerdos pactados en el BCM: se realizan ejercicios, simulaciones o análisis paso a paso con el fin de probar el plan y evaluar la oportunidad de mejora.
 - **Etapa 6.** Cultura organizacional: se debe mantener el liderazgo y fomentar la unión de todos los empleados y miembros de la organización pues son parte del buen funcionamiento y en parte, de ellos depende el buen funcionamiento del plan.



Figura 6. Equipo de trabajo.
(Shutterstock 2021).



04

PLAN DE RECUPERACIÓN ANTE DESASTRES (PRD)

La norma internacional ISO 22301 ha sido creada en 2012 en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas. La ISO 22301 identifica las bases de un sistema de gestión de la continuidad del negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio en caso de un desastre.

Este marco garantiza la continuidad de operaciones de todo tipo y tamaño de organizaciones, protegiendo a sus empleados y a la infraestructura y manteniendo en todo momento su reputación.

La norma ISO 22301 puede ser aplicada a:

- Establecer, implantar, mantener y mejorar un SGCN.
- Demostrar conformidad con la política establecida de la continuidad de negocio de la organización.
- Dar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas internacionalmente.

La norma ISO 22301 identifica los riesgos y determina cómo puede afectar la continuidad de la empresa, a fin de generar respuestas adecuadas y rápidas al momento de una crisis. La norma también permite la cooperación entre empleados, mejora la reputación y le da un valor agregado a la empresa al contar con la certificación.



Para la aplicación de esta norma internacional se debe documentar:

- El alcance que tendrá la norma y la lista de requisitos legales, normativos y de otra índole.
- Política de la continuidad de negocio, incluyendo los objetivos de la continuidad del negocio.
- Competencias del personal y las vías de comunicación con las partes interesadas.
- Análisis del impacto en el negocio y del riesgo.
- Planes de continuidad del negocio y la estructura de la respuesta ante incidentes detallando cada parte del proceso.
- Resultados de acciones preventivas.
- Auditoría interna.
- Acciones correctivas.
- Mejora continua.





05

AUDITORÍA

En el contexto de la ciberseguridad y el Big Data, la auditoría de la base garantiza la seguridad de la data al monitorear y registrar las acciones configuradas de la base de datos de usuarios y no usuarios.

Se deben auditar tanto las actividades exitosas como las fallidas. Los auditores pueden incluir o excluir a usuarios específicos de la auditoría si así lo consideran. Una auditoría puede ser una acción individual o en combinación de datos, siendo este un proceso continuo.

Los principales tipos de actividades de riesgo incluyen:

Error: la falta de mantenimiento en la base de datos puede originar la divulgación accidental de información. Los cambios no autorizados dan lugar a divulgaciones, inserciones, actualizaciones o eliminaciones accidentales y no autorizadas.

Uso indebido: una falla en el mantenimiento de los derechos de acceso a la base de datos conduce a su abuso y puede causar una filtración de información.

Acción maliciosa: el robo de datos o un ataque de denegación de servicio (DoS) puede ocurrir si no se mantiene una configuración lógica y segura de la base de datos.

El análisis de la configuración de la base de datos es fundamental para determinar las vulnerabilidades y garantizar la auditoría estándar. Toda auditoría de la base de datos incluye:

- Encontrar privilegios y datos confidenciales.
- Impedir el acceso a los datos.
- Validar que los mecanismos de detección y alerta estén en su lugar.



Se disponen de varios mecanismos que deben estar en su lugar cuando se configuran las bases de datos, algunos de ellos son:

- **La redacción de datos:** proporciona una redacción selectiva y al momento de los datos confidenciales en los resultados de las consultas SQL y antes de la visualización de la aplicación, de esta manera evita que los usuarios no autorizados puedan ver los datos confidenciales. La redacción de datos no tiene ningún impacto en las actividades operativas de la base de datos.
- **El enmascaramiento de datos:** reemplaza los datos confidenciales con otros datos, con ello asegura que la información de identificación personal se oculte.
- **El cifrado de datos:** transforma los datos en texto cifrado codificado, a menudo ilegible, utilizando algoritmos y cálculos matemáticos no legibles. Para restaurar el mensaje se requiere un algoritmo de descifrado correspondiente y la clave de cifrado original. Es fundamental en tarjetas de crédito.

5.1. PASOS DE AUDITORÍA DE LA BASE DE DATOS

Primero hay que definir el alcance y complejidad de la auditoría antes de la ejecución de las actividades. Es conveniente especificar previamente la intención que se tenga con los resultados y sus conclusiones a fin de establecer las necesidades. De forma general, se deben seguir los siguientes pasos para la auditoría de la base de datos:

1. Planeación de la auditoría

Ante todo, se autoriza la realización de la auditoría y se conforma el equipo de auditoría. Posteriormente se especifican las fechas para llevar a cabo la revisión, en concordancia con la planeación de las actividades del sistema de gestión.

El equipo de auditoría puede estar conformado por profesionales de diversas áreas e incluye un auditor líder, uno o más auditores adjuntos y varios observadores. Su primera tarea es establecer los objetivos y el alcance a fin de gestionar los recursos necesarios. Igualmente, se debe seleccionar criterios de auditoría para continuar con el siguiente paso.



Figura 7. Auditoría.
(Shutterstock 2021).



Figura 8. Revisión de documentos.
(Shutterstock 2021).

2. Revisión documental

Antes de la ejecución de las actividades de la auditoría se requiere la revisión de la documentación del sistema de gestión a partir de los criterios definidos en el paso previo. El propósito de esta etapa es contar con una visión amplia del contexto para identificar los elementos de interés.

3. Preparación de auditoría en sitio

El equipo planifica todas las actividades necesarias para la revisión en sitio, incluyendo las listas de verificación que les permitirán identificar el alcance de la auditoría y los objetivos.

Algunas de las actividades que se pueden realizar como parte de la auditoría son:

- Auditoría de la configuración de las cuentas buscando que sus contraseñas sean únicas y seguras.
- Auditoría de la solidez del SID de la base de datos.
- Auditoría de las actualizaciones de parches críticos.
- Auditoría de la función pública para la identificación de privilegios innecesarios.
- Auditoría de que se realicen evaluaciones periódicas de seguridad de la base de datos.
- Auditoría de que el tráfico de la base de datos está cifrado.
- Auditoría de las amenazas y contramedidas de seguridad.

4. Auditoría en sitio

Teniendo un plan de acción estipulado en los pasos previos, el equipo de auditoría se dirige al sitio y ejecuta el protocolo de auditoría con eficiencia. Durante esta etapa se hace una junta de apertura donde se resuelven las dudas y se presenta al equipo, luego se procede a la auditoría en sitio (observaciones, entrevistas y revisiones) y una vez que finalice se deben comunicar los hallazgos que quedarán asentados en la junta de cierre.



Figura 9. Auditoría en el sitio.
(Shutterstock 2021).

5. Conclusiones de la auditoría

Durante la junta de cierre se solucionan las dudas y particularidades del proceso en presencia del equipo auditor y del auditado, este último debe firmar en conformidad y posteriormente presentar al equipo auditor un plan para resolver las no conformidades y observaciones encontradas.

El informe de auditoría debe ser elaborado por el equipo plasmando los resultados y resoluciones emitidas durante el proceso. Previo a su publicación, este informe debe ser aprobado por el auditor líder y debe ser presentado a las partes interesadas durante la junta de cierre. Por último, se publicará el informe a través del medio de comunicación establecido en la junta de apertura.



6. Seguimiento de la auditoría

Concluido con las actividades de auditorías, se puede realizar un seguimiento sobre las acciones correctivas que presente el auditado. Recordemos que las auditorías son procesos continuos y que funcionan para analizar el estado actual del sistema y mantenerlo seguro y confiable.





06

BIG DATA EN EL ÁMBITO DE LA CIBERSEGURIDAD

Ante el aumento del cibercrimen resulta imperante la inversión en ciberseguridad por parte de las empresas. En tanto, surge un nuevo concepto la ciberinteligencia definida como “la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoyen la toma de decisiones”. Es decir, la ciberinteligencia extrae información del análisis de los datos obtenidos y permite rastrear y neutralizar las ciberamenazas, mientras disminuye y refuerza las debilidades.

Anteriormente los analistas de seguridad debían estudiar los incidentes informáticos de forma manual. En la actualidad se hace uso de la Data Science y la Inteligencia Artificial para identificar patrones que antes no se podían. El reto ahora está en el debido almacenamiento de la Big Data de una manera eficiente que permita toda la analítica de seguridad correspondiente.

El machine learning se encarga de aplicar métodos estadísticos y matemáticos para hacer que los equipos del SOC (Security Operations Center) aprendan y ejecuten tareas de seguridad, sin necesidad de ser programadas explícitamente, logrando la detección de incidentes previamente no detectados o de predecir las posibles amenazas.



Conclusión

La ciberseguridad se aplica a todos los entornos, empresas u organismos de todo tipo y magnitud. El capital esencial es el humano, proteger sus datos y generar confianza es primordial para establecer una marca que perdure en el tiempo, la ciberseguridad conecta personas, la cooperación nos hace más eficientes.

La información tiene un valor incalculable y la vulnerabilidad es el peor enemigo. Con la transformación digital y el incremento de la tecnología se automatizan muchos procesos, pero se incrementan las amenazas. Ante este panorama el análisis y la gestión de riesgos permite minimizar los efectos adversos que pueden ocurrir. En conjunto con la continuidad de negocios, las normas internacionales y las políticas se establece un plan de acción rápido y eficiente ante los ataques que puedan comprometer la data y a su vez, la reputación de la empresa.

La Big Data va concatenada a la seguridad de la información y da paso a la ciberinteligencia, En fin, el manejo de estas herramientas permite comprender mejor a los clientes, optimizar procesos y mejorar el rendimiento de una empresa.





BIBLIOGRAFÍA

AUDITORÍA DE CÓDIGO. “*El arte del desarrollo seguro (diseño seguro)*”. (2021, 24 abril). <https://auditoriadecodigo.com/desarrollo-seguro-es-diseno-seguro/>

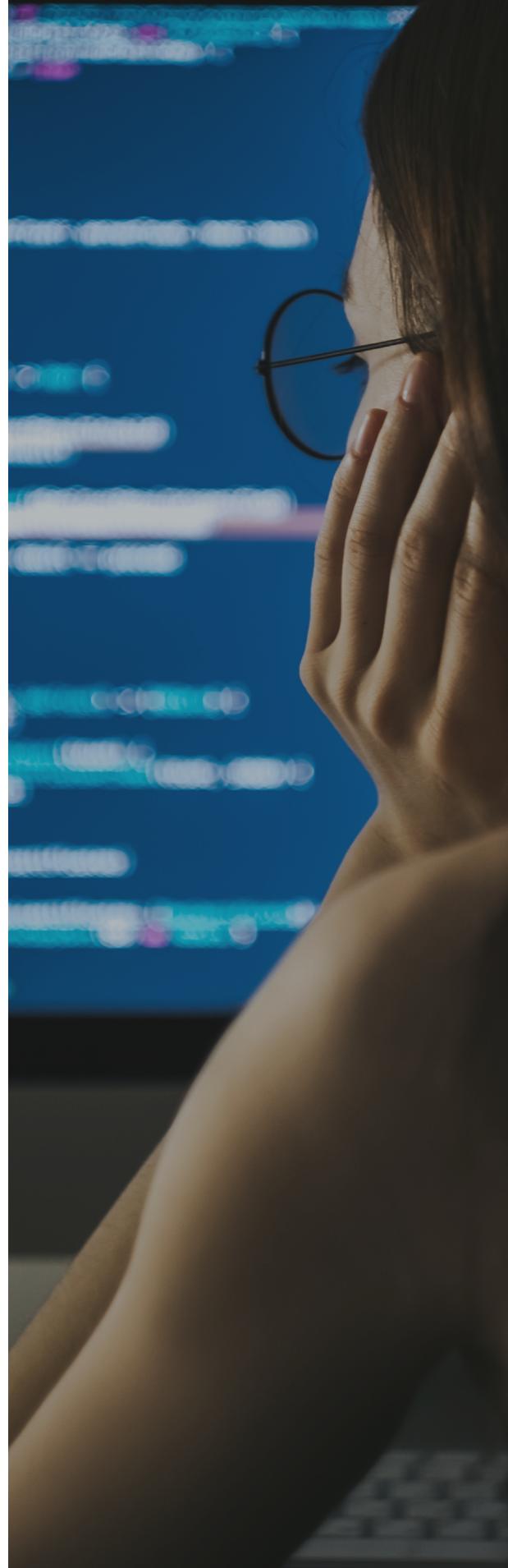
DATAHACK. “**LAS 10 V'S DEL BIG DATA**”. (2020, 12 noviembre). <https://www.datahack.es/blog/big-data/10-vs-del-big-data/>

ESCUELA EUROPEA DE EXCELENCIA. (2018, 16 mayo). “*Cómo realizar la evaluación de riesgos según ISO 31000:2018*”. <https://www.escuelaeuropeaexcelencia.com/2018/05/como-realizar-la-evaluacion-de-riesgos-segun-iso-310002018/>

ISACA “AUDITING ORACLE DATABASES”. (2014, 1 noviembre).. <https://www.isaca.org/resources/isaca-journal/past-issues/2014/auditing-oracle-database>

KARL THOMAS. (2015, 24 agosto). *Los usuarios de Ashley Madison, “blancos fáciles para la extorsión”*. <https://www.welivesecurity.com/la-es/2015/08/24/usuarios-ashley-madison-blancos-extorsion/>

LÓPEZ, A. (S. F.). ISO 27001. ISO 27000. es. Recuperado 7 de julio de 2021, de https://www.iso27000.es/iso27002_5.html





OCHOA VÁSQUEZ, J. M. (2020, noviembre). Aplicando data science, análisis de datos e inteligencia artificial a ciberinteligencia. Máster en data science y análisis de datos. Instituto Europeo de Estudios Empresariales.

STEPHEN COBB. (2014, 14 mayo). “*4 pasos para armar un Plan de Continuidad del Negocio que asegure el futuro digital de la empresa*”. <https://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/>

TRANSFORMING DATA WITH INTELLIGENCE. (2017, 8 febrero). “*The 10 Vs of Big Data.*” <https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx>

ISO 22301. (2019, 29 abril). Software ISO. <https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301/>

ISO 31000:2018. (2018). Software ISO. <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en>



ADEN

