INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 14

12 DE DICIEMBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Son herramientas que abarcan desde la revisión hasta la evaluación de la seguridad desde todos los ámbitos técnicos, tecnológicos y organizativos de la seguridad.-

¿Qué es?

Las auditorías técnicas son procesos de evaluación sistemática y objetiva de sistemas, aplicaciones, infraestructuras, procesos o cualquier otro componente técnico dentro de una organización. El objetivo principal de una auditoría técnica es verificar y asegurar que los sistemas y procesos cumplen con los estándares establecidos, políticas internas, normativas externas y mejores prácticas de seguridad, rendimiento y eficiencia.

Estas auditorías suelen ser llevadas a cabo por profesionales especializados en el área técnica, como auditores de sistemas, ingenieros de seguridad informática o expertos en la materia correspondiente.

Funciones

Evaluación de Seguridad:

- Identificación y evaluación de vulnerabilidades en sistemas y aplicaciones.

- Análisis de controles de seguridad para garantizar el cumplimiento de políticas y estándares.

Cumplimiento Normativo:

- Verificación de que los sistemas y procesos cumplen con normativas y regulaciones específicas.

- Aseguramiento de que se siguen las mejores prácticas y estándares de la industria.

Rendimiento y Eficiencia:

- Evaluación del rendimiento de sistemas y aplicaciones.

- Identificación de posibles mejoras para aumentar la eficiencia operativa.

Revisión de Infraestructura:

- Análisis de la arquitectura de red y sistemas.

- Evaluación de la redundancia y disponibilidad de la infraestructura tecnológica.

Calidad del Código:

- Revisión del código fuente de aplicaciones para identificar errores y problemas de codificación.

- Garantía de que se sigan las mejores prácticas de desarrollo.

Gestión de Riesgos:

- Identificación y evaluación de riesgos asociados con los sistemas y procesos.

- Desarrollo de estrategias para mitigar y gestionar los riesgos identificados.

Documentación Técnica:

- Revisión de la documentación técnica para garantizar su precisión y actualización.

- Identificación de posibles brechas en la documentación.

Seguimiento de Incidentes:

- Revisión de la gestión de incidentes de seguridad.

- Análisis de la respuesta y recuperación frente a eventos adversos.

Tipos

Algunos tipos de auditorias técnicas pueden ser:

- Auditoría de Seguridad Informática: Evaluación de la seguridad de sistemas, redes y datos para identificar vulnerabilidades y riesgos.

- Auditoría de Sistemas y Aplicaciones: Revisión de la arquitectura y el rendimiento de sistemas y aplicaciones para garantizar eficiencia y cumplimiento de requisitos.

- Auditoría de Cumplimiento Normativo: Verificación de que la organización cumple con las normativas y regulaciones específicas aplicables.

- Auditoría de Continuidad del Negocio: Evaluación de la capacidad de la organización para mantener operaciones críticas durante interrupciones o desastres.

- Auditoría de Infraestructura de Red: Análisis de la estructura de la red para asegurar eficiencia, seguridad y disponibilidad.

- Auditoría de Base de Datos: Revisión de la seguridad, integridad y eficiencia de las bases de datos de la organización.

- Auditoría de Calidad del Código: Examen del código fuente de aplicaciones para identificar errores, vulnerabilidades y asegurar las mejores prácticas de programación.

- Auditoría de Gestión de Identidad y Acceso: Evaluación de la gestión de identidades y los controles de acceso para garantizar la seguridad de los sistemas y la información.

Recomendaciones

Garantizar la actualización constante de nuestras herramientas tecnológicas es esencial para mantener nuestros sistemas al día y resguardados contra posibles amenazas como virus y vulnerabilidades. Contar con empresas y profesionales especializados nos proporciona información confiable y verificada sobre la seguridad en nuestra organización, así como frente a cualquier incidente de seguridad.

Además, es crucial concientizar a nuestros empleados acerca de la importancia de utilizar correctamente los sistemas corporativos. Esto implica evitar la instalación de software no autorizado, abstenerse de navegar por páginas web de contenido dudoso y, en general, cumplir con todas las disposiciones establecidas en la política de seguridad de la empresa. De esta manera, fortalecemos nuestras defensas y reducimos el riesgo de ataques y malware.

Escenario de aplicación

El IES Celia Viñas, un centro educativo moderno, utiliza tecnologías avanzadas para facilitar la enseñanza y la administración. La infraestructura tecnológica incluye sistemas de gestión académica, redes inalámbricas, laboratorios de informática y una plataforma en línea para la interacción estudiante-profesor.

1. Auditoría de Seguridad Informática:

El departamento de tecnología del IES Celia Viñas realiza auditorías de seguridad informática de forma regular. Los expertos en seguridad evalúan la red, los sistemas y las aplicaciones educativas para identificar posibles vulnerabilidades y garantizar la protección de la información sensible de estudiantes y profesores.

2. Auditoría de Sistemas y Aplicaciones:

Se lleva a cabo una auditoría de sistemas y aplicaciones para evaluar la eficiencia y funcionalidad de las plataformas educativas. Esto asegura que los recursos digitales estén optimizados para mejorar la experiencia de aprendizaje y facilitar la labor docente.

3. Auditoría de Cumplimiento Normativo:

El centro educativo se somete a auditorías para asegurar el cumplimiento de normativas educativas y regulaciones de protección de datos. Esto garantiza que las prácticas educativas digitales estén alineadas con las leyes vigentes.

4. Auditoría de Infraestructura de Red:

La infraestructura de red se evalúa para garantizar una conectividad estable y segura. La auditoría aborda aspectos como la capacidad de la red, la redundancia y la disponibilidad para respaldar la enseñanza en línea y otras actividades digitales.

5. Auditoría de Calidad del Código (Desarrollo de Aplicaciones Educativas):

Cuando se desarrollan aplicaciones educativas personalizadas, se realiza una auditoría de calidad del código. Esto asegura que las aplicaciones sean seguras, eficientes y cumplan con los estándares de desarrollo.

6. Sesiones de Concientización para Estudiantes y Personal:

Se organizan sesiones de concientización para estudiantes y personal docente sobre buenas prácticas en seguridad informática. Esto incluye instrucciones sobre el uso adecuado de las tecnologías, evitando la descarga de software no autorizado y practicando una navegación segura.