cyber zaintza
BASQUE CYBERSECURITY AGENCY

Servicio de auditorías técnicas de ciberseguridad

EUSKO JAURLARITZA
GOBIERNO VASCO

Índice

1. Introducción 3
2. Metodología de evaluación 4
   2.1. Fases de la metodología de evaluación 4
      2.1.1. Preparación y planificación 4
      2.1.2. Lanzamiento 5
      2.1.3. Ejecución 6
      2.1.4. Documentación 6
3. Tipología de auditorías de seguridad 8
   3.1. Auditoría de seguridad de aplicaciones web 8
   3.2. Auditoría de seguridad de aplicaciones móviles 8
   3.3. Auditoría de seguridad de red externa 9
   3.4. Auditoría de seguridad de red interna 9
   3.5. Auditoría de seguridad de redes WIFI 10
   3.6. Auditoría de seguridad de información accesible desde Internet 10
   3.7. Auditoría de directorio activo 11
   3.8. Auditoría de configuración de dispositivos de protección 12

1.Introducción

Este documento tiene como objetivo detallar de manera clara el funcionamiento del servicio de auditorías técnicas prestado por Cyberzaintza a sus diferentes públicos objetivo.

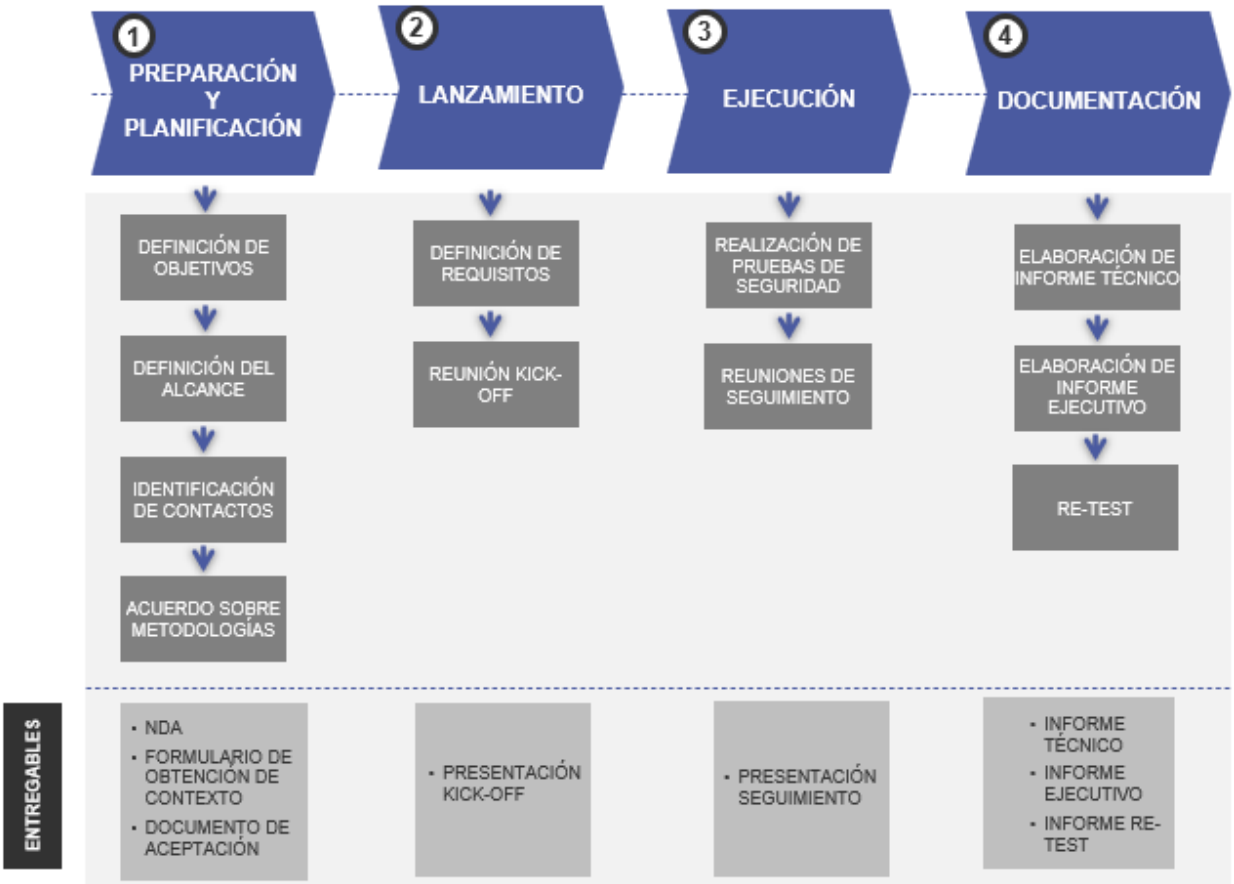
Las entidades a las que Cyberzaintza ofrece el servicio de auditorías técnicas de ciberseguridad pueden solicitar la prestación del mismo enviando un email a auditec@cyberzaintza.eus. En ese momento, el equipo a cargo del servicio envía el presente documento informativo en el que se especifican las fases y tareas generales que engloba la prestación del servicio, así como la descripción de la tipología de auditorías que se pueden solicitar.

2. Metodología de evaluación

El servicio de auditorías técnicas tiene como objetivo identificar vulnerabilidades, riesgos y áreas de mejora en la infraestructura tecnológica de las organizaciones. Para ello, se utilizará un enfoque basado en los estándares internacionales para garantizar una evaluación exhaustiva y objetiva de los sistemas, redes y aplicaciones.

2.1. Fases de la metodología de evaluación

A continuación, se detallan las fases que se siguen durante las auditorías técnicas, para asegurar el cumplimiento de los objetivos detallados anteriormente:



2.1.1. Preparación y planificación

La primera fase consta de la preparación y planificación de la auditoría que se solicite. En esta fase, se llevarán a cabo diversas tareas fundamentales para el desarrollo de la actividad:

- **Definición de objetivos**: se acuerda con la entidad los objetivos concretos de la auditoría.
- **Establecimiento del alcance**: se delimita exactamente qué sistemas, subredes o servicios entran dentro del alcance de la auditoría.
- **Identificación de contactos**: se recogen los datos de las personas de referencia que serán los responsables de gestionar las incidencias y recibir las notificaciones de vulnerabilidades críticas que necesiten corrección inmediata.
- **Acuerdo sobre metodologías**: se revisan y validan las metodologías de trabajo que se van a emplear en función del tipo de auditoría, así como el tipo de pruebas.

Los entregables a los que dará lugar esta fase son:

- **NDA**: acuerdo de confidencialidad firmado por ambas partes para proteger la información sensible durante todo el proceso.
- **Formulario de obtención de contexto de la entidad**: documento en el que la entidad proporciona detalles sobre arquitecturas, tecnologías usadas y todos los datos que se consideren necesarios.
- **Documento de aceptación**: documento en el que la entidad acepta los términos finales del alcance, fechas, horarios autorizados, IPs de origen de las pruebas y condiciones acordadas.

2.1.2. Lanzamiento

Durante la fase de lanzamiento, previa a la realización de las pruebas, se realizan las siguientes tareas:

- **Definición de requisitos**: se concretan los requisitos técnicos y operativos finales: IP públicas desde las que se realizarán los escaneos, accesos VPN, etc. Se validan las credenciales aportadas y las conexiones remotas para comprobar que todo está correctamente configurado.
- **Reunión de kick-off**: se realizará una reunión entre los responsables de la entidad y el equipo auditor de Cyberzaintza para repasar los objetivos y alcance definidos, calendarización de las pruebas, presentación de roles, responsabilidades y contactos y se resolverán las dudas que puedan surgir.

En esta fase, surgen los siguientes entregables:

- **Presentación del kick-off**: diapositivas que recopilan lo tratado en la reunión.

2.1.3. Ejecución

En la fase de ejecución se llevarán a cabo las pruebas de seguridad acordadas previamente, junto con otras tareas que se detallan a continuación:

- **Realización de pruebas de seguridad**: se llevan a cabo las actividades de pentesting propiamente dichas: reconocimiento, identificación de vulnerabilidades, explotación controlada y pruebas de post-explotación.
- **Reuniones de seguimiento**: a petición de la entidad, a intervalos predefinidos se realizarán reuniones de seguimiento del proceso para informar a nivel general sobre el estado de las pruebas y los hallazgos encontrados hasta el momento.

Los entregables generados en esta fase son:

- **Presentaciones de reuniones de seguimiento**: diapositivas en las que se informa el estado general de la auditoría y el resumen de los avances.

2.1.4. Documentación

La última fase trata de la fase de documentación, donde se termina de documentar el proceso y los hallazgos, se realiza la entrega de los mismos para su revisión, y se acuerda y realiza un re-test en el caso de que la entidad lo solicite.

- **Elaboración del informe técnico**: informe en el que se explican detalladamente las pruebas realizadas, la metodología utilizada, el listado completo de vulnerabilidades y recomendaciones de remediación específicas.
- **Elaboración del informe ejecutivo**: documento más conciso, orientado a mandos directivos con un lenguaje menos técnico.
- **Re-test**: en el caso de que la entidad lo solicite, se concretarán fechas para la resolución de un re-test y se ejecutará en la calendarización estimada, generando posteriormente un apartado adicional a introducir en el informe técnico.

Los documentos a entregar que surgen de esta fase son:

- **Informe técnico**.

- **Informe ejecutivo.Informe técnico con apéndice de re-test.**

3. Tipología de auditorías de seguridad

A continuación, se describen los distintos tipos de auditorías técnicas que se prestan dentro del alcance del servicio, proporcionando una visión general de cada una de ellas.

3.1. Auditoría de seguridad de aplicaciones web

La auditoría de seguridad de **aplicaciones web** tiene como objetivo principal identificar vulnerabilidades y riesgos potenciales que puedan poner en peligro la integridad, confidencialidad y disponibilidad de la misma, así como de los datos que maneja.

Para llevarla a cabo, se utilizan diversos enfoques, siendo estos:

- **Análisis de caja negra:** se simula un ataque externo sin conocimientos previos, ni acceso a la aplicación.
- **Análisis de caja gris:** se otorga credenciales limitadas para auditar con un acceso controlado.
- **Análisis de caja blanca:** se proporciona acceso total a la información y código de la aplicación para una evaluación exhaustiva.

La metodología empleada para la auditoría es el **WSTG** (**Web Security Testing Guide**), un marco de trabajo reconocido y ampliamente utilizado en el ámbito de la ciberseguridad. Este enfoque proporciona una serie de directrices y prácticas estandarizadas para realizar pruebas de seguridad exhaustivas en aplicaciones web.

3.2. Auditoría de seguridad de aplicaciones móviles

La auditoría de seguridad de **aplicaciones móviles** se centra en evaluar la seguridad de estas, con especial atención a las comunicaciones que establece con otros servicios remotos.

Al inicio de la auditoría de seguridad de aplicaciones móviles, se emplea un enfoque caja negra, donde el auditor simula un atacante externo sin acceso previo a la aplicación. Si el proceso de autenticación falla, se utiliza un enfoque caja gris, otorgando credenciales limitadas para acceder a áreas privadas y continuar con el análisis interno de la aplicación.

Para garantizar una evaluación precisa y eficaz en las auditorías de aplicaciones móviles, seguimos una metodología adaptada específicamente a las necesidades de seguridad de

cada aplicación, utilizando **OWASP MAS** (**Mobile Application Security Testing**) como base. Esta metodología tiene en cuenta las características particulares de la aplicación móvil, su arquitectura, los posibles riesgos asociados y los objetivos de seguridad establecidos por el cliente. Al aplicar las directrices y mejores prácticas de OWASP MAS, nos aseguramos de realizar una evaluación exhaustiva de la seguridad de la aplicación, identificando vulnerabilidades y riesgos específicos, y proporcionando recomendaciones claras para mitigar posibles amenazas.

3.3. Auditoría de seguridad de red externa

La **auditoría externa**, basada en un test de intrusión a los activos expuestos de la entidad desde Internet, tiene como objetivo principal identificar debilidades en los sistemas, elementos de red y comunicaciones, así como evaluar la accesibilidad y visibilidad de los sistemas y las redes.

Realizar una auditoría de infraestructura externa permite identificar vulnerabilidades críticas en sistemas expuestos a Internet, simulando ataques reales para evaluar posibles brechas de seguridad. Esto ayuda a fortalecer las defensas perimetrales, mejorar la protección de datos y garantizar el cumplimiento de normativas.

La metodología empleada para realizar una auditoría de infraestructura externa sigue un enfoque metódico y estructurado, basado en estándares reconocidos como **PTES** (**Penetration Testing Execution Standard**) u **OSSTMM** (**Open Source Security Testing Methodology Manual**), diseñado para evaluar de manera exhaustiva la seguridad de los sistemas y redes accesibles desde el exterior.

3.4. Auditoría de seguridad de red interna

La auditoría de seguridad de una **red interna** tiene como objetivo evaluar y mejorar la protección de los sistemas y dispositivos dentro de una infraestructura corporativa. Este proceso se enfoca en identificar posibles vulnerabilidades en redes, servidores, aplicaciones y dispositivos conectados, con el fin de detectar riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad de la información.

Al realizar esta auditoría, se proporciona una visión clara de la seguridad interna, detectar fallos de configuración y reforzar las políticas de acceso y control de la red para evitar intrusiones y ataques internos.

Para llevar a cabo esta auditoría, se utilizan metodologías estructuradas y probadas como **OWASP** (**Open Web Application Security Project**), **NIST** (**National Institute of Standards and Technology**) y **MITRE ATT&CK**, que proporcionan marcos de trabajo detallados para evaluar la seguridad de la red y los sistemas internos. Estas metodologías permiten realizar un análisis exhaustivo a través de fases como la recopilación de información, el escaneo de vulnerabilidades, la explotación controlada de fallos de seguridad y las pruebas de resistencia ante posibles ataques.

3.5. Auditoría de seguridad de redes WIFI

La auditoría de seguridad de **redes Wi-Fi** tiene como objetivo identificar y mitigar vulnerabilidades dentro de las redes inalámbricas de una organización. Este proceso se enfoca en evaluar la configuración de los puntos de acceso, el tipo de cifrado utilizado, las políticas de autenticación y los posibles riesgos asociados con dispositivos no autorizados o accesos no controlados.

Al realizar esta auditoría, se busca garantizar que la red Wi-Fi sea resistente a ataques como el sniffing de tráfico, la interceptación de datos o la suplantación de identidad, protegiendo así la confidencialidad e integridad de la información transmitida.

Para realizar una auditoría exhaustiva de redes Wi-Fi, se emplean metodologías específicas para redes inalámbricas. Estas metodologías, como **OWISAM** (**Open Wireless Security Assessment Methodology**), incluyen técnicas como la recopilación de información sobre puntos de acceso, pruebas de cifrado (WEP, WPA2, WPA3), ataques de denegación de servicio (DoS) y la validación de configuraciones de seguridad.

3.6. Auditoría de seguridad de información accesible desde Internet

La auditoría de **información accesible desde Internet** (OSINT, Open Source Intelligence) se enfoca en recopilar y analizar información pública disponible a través de fuentes accesibles en Internet. Este proceso tiene como objetivo identificar datos sensibles que puedan ser

utilizados de manera malintencionada por atacantes, como direcciones de correo electrónico, nombres de usuario, detalles de infraestructura y vulnerabilidades expuestas.

A través de una investigación meticulosa, se busca evaluar el nivel de exposición de una organización en Internet, proporcionando una visión clara de qué información está accesible públicamente y cómo podría ser explotada.

Para llevar a cabo esta auditoría, se utilizan metodologías específicas de recolección de inteligencia abierta como **OSINT Framework**, empleando herramientas especializadas que permiten explorar diversas fuentes, como redes sociales, bases de datos filtradas, registros WHOIS, y otros recursos públicos, con el fin de obtener información detallada sobre la organización objetivo.

3.7. Auditoría de directorio activo

Las auditorías de **directorio activo** son esenciales para garantizar que los sistemas de autenticación y autorización dentro de una organización estén correctamente configurados y protegidos contra accesos no autorizados.

El directorio activo (Active Directory, AD) es una herramienta fundamental en la gestión de usuarios y recursos en redes corporativas, y su seguridad es crucial para prevenir amenazas internas y externas. Mediante una auditoría de directorio activo, se evalúa cómo se gestionan las cuentas de usuario, los privilegios de acceso y las políticas de seguridad, identificando posibles vulnerabilidades que puedan ser explotadas por atacantes para obtener acceso no autorizado a sistemas críticos.

Durante una auditoría de directorio activo, se revisa la estructura de grupos y permisos, asegurándose de que las políticas de acceso sean adecuadas y estén alineadas con los principios de mínima privilegio y separación de funciones. Se analizan las configuraciones de contraseñas, el uso de autenticación multifactor y la correcta implementación de directivas de seguridad para proteger contra el acceso no autorizado. Además, se verifica la existencia de cuentas inactivas, configuraciones débiles en las políticas de seguridad y posibles brechas en la auditoría de eventos, que podrían permitir que un atacante escale privilegios dentro de la red corporativa.

La metodología de la auditoría de directorio activo involucra una serie de pasos estructurados que siguen como base el estándar **PTES** (**Penetration Testing Execution Standard**). A través

de herramientas especializadas y técnicas de prueba de penetración, se simulan posibles escenarios de ataque para identificar puntos débiles y ofrecer recomendaciones prácticas para mejorar la seguridad. Con estos resultados, las entidades pueden reforzar su directorio activo, proteger los datos sensibles y minimizar el riesgo de acceso no autorizado.

3.8. Auditoría de configuración de dispositivos de protección

Las auditorías de **configuración de dispositivos de protección**, como firewalls, sistemas de prevención de intrusiones (IPS), sistemas de detección de intrusiones (IDS), y soluciones de detección y respuesta en endpoints (EDR), son fundamentales para asegurar que los sistemas de seguridad de una entidad estén correctamente configurados y operando de manera efectiva. Estos dispositivos actúan como barreras de defensa cruciales contra amenazas externas e internas, por lo que su correcta configuración y mantenimiento es esencial para proteger la infraestructura tecnológica y la información sensible.

Durante la auditoría, se revisan aspectos clave como las reglas y políticas del firewall, la configuración de los sistemas IPS/IDS para detectar y prevenir ataques en tiempo real, y la implementación de soluciones EDR para identificar y responder rápidamente a incidentes de seguridad en los endpoints. Se evalúa si las políticas de acceso, monitoreo y análisis de tráfico están correctamente definidas, si los dispositivos están actualizados con las últimas firmas de amenazas y si se han configurado correctamente las alertas para una respuesta oportuna. Además, se verifica que no existan configuraciones inseguras, como puertos abiertos innecesarios o reglas excesivamente permisivas, que puedan abrir brechas de seguridad en la red.

La metodología de una auditoría de configuración de dispositivos de protección incluye la revisión exhaustiva de las configuraciones actuales, la simulación de ataques para evaluar la efectividad de la defensa y el análisis de los registros de eventos generados por estos dispositivos. Esta revisión se basa en estándares reconocidos como los **CIS Benchmarks** (**Center for Internet Security**), que proporcionan guías detalladas para validar que las configuraciones cumplan con las mejores prácticas de seguridad. Los resultados se resumen en un informe detallado que incluye recomendaciones para optimizar las configuraciones de seguridad, mejorar la visibilidad de la red y garantizar que los dispositivos de protección estén alineados con los marcos de referencia más robustos del sector.

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza
BASQUE CYBERSECURITY AGENCY

¡Muchas gracias!

www.ciberseguridad.eus