“Universidad Internacional de La Rioja en México”

Desarrollo Seguro de Software y Auditoría de la Ciberseguridad

Proyecto:

Actividad: Plan de una auditoría técnica de seguridad de una empresa

Profesor:

Francisco Javier Álvarez Solis

Autor:

Juan Luis Cruz Aristeo.

Fecha de entrega:

27/01/2025

Índice

Introducción

En la actualidad la seguridad de los sistemas de información se ha vuelto un factor clave y crítico, para todas las organizaciones. Esto se debe a que, en la actualidad, las operaciones de las empresas y organizaciones dependen en gran medida de las tecnologías de la información. Ya que hoy en día, existen plataformas, software y sistemas complejos que permiten a las empresas y organizaciones llevar a cabo sus operaciones de manera más eficiente y efectiva. Estas tecnologías permiten la automatización de procesos, el análisis de grandes cantidades de datos, la comunicación instantánea, la colaboración en tiempo real y la migración de procesos físicos a digitales, tales como los tramites de gobierno. Sin embargo, esta dependencia de la tecnología trae consigo riesgos potenciales, ya que los sistemas de información pueden ser vulnerables a ataques cibernéticos, violaciones de datos, errores de software y demás tipos de incidentes de seguridad.

Es así que el objetivo de este proyecto es realizar un plan de auditoría, para poder aplicarla en la experiencia reciente de la librería On-line S.A. En la cual un ciberataque comprometió las credenciales de sus usuarios y cuota de mercado. Este incidente pone en el plano la importancia de tener una infraestructura tecnológica segura y cumplir con las normativas de protección de datos. Por lo tanto, para cumplir con las normativas se diseñará un plan de auditoria técnica de seguridad. Este análisis detallado abarcara los sistemas, redes, aplicaciones y procesos de la organización, con el fin de identificar vulnerabilidades existentes y proponer algunas salva guardas para mitigarlas.

De esta forma, para poder lograr este objetivo, habrá que diseñar primero el plan de auditoria técnica de seguridad el cual incluirá los siguientes puntos.

- Propósito de la auditoría.
- Objetivos de la auditoría.
- Alcance de la auditoría técnica de seguridad.
- Metodologías.
- Programa de trabajos (planificación)

- Organización y recursos necesarios.
- Entregables (tipos de informes a entregar y apartados).
- Procedimientos de comunicación con los responsables de proyecto.
- Presupuesto e hitos de facturación.
- Evaluación de riesgos del proyecto.
- Anexo I: Acuerdo de autorización.

Contexto

La librería ha sufrido un ciberataque que ha comprometido las credenciales de sus clientes. El incidente ha trascendido a los medios de comunicación, lo que ha producido una pérdida de cuota de mercado importante frente a sus competidores.

Con el objetivo de mantener su actual posición en el mercado de venta electrónica de libros y volver a recuperar e incluso superar la que tenía, ha contratado a la empresa InfoSecurity para llevar a cabo una auditoría técnica de seguridad a todos sus sistemas TI e implementar las salvaguardas que se deriven del mismo en función del nivel de riesgo y la disponibilidad económica.

La librería dispone de una tienda web en la que el cliente necesitará autenticarse con las credenciales de la cuenta de usuario, que a su vez se comprobarán con la base de datos implementada en el backend de la compañía a través de una interfaz de servicios web.

Se dispone de un procesamiento de tarjetas de crédito subcontratado a un procesador de terceros. El sitio web se desplegará en Internet protegido por una DMZ de dos capas con acceso tanto para usuarios internos como externos.

Se tendrá que elaborar un plan de auditoría para la realización de la citada auditoría técnica de seguridad de la siguiente infraestructura TIC de la organización compuesta de los siguientes elementos:

- ☐ Accesos externos VPN.
- ☐ Zona DMZ: FW y IDS.
- ☐ Publicación sitio web de la empresa.
- ☐ Correo externo e interno.
- ☐ Servicio públicos DNS y FTP.
- ☐ Infraestructura de red: router y switch.
- ☐ Aplicaciones internas Intranet y aplicaciones corporativas.
- ☐ Zona wifi.

- ☐ Segmentación en VLAN de la red interna: servidores y usuarios.
- ☐ Sistema AAA (autenticación, autorización y trazabilidad).
- ☐ Sistema de antimalware.
- ☐ Aplicación web de la empresa expuesta al exterior.

Propósito de la auditoria

De esta forma el propósito principal de esta auditoria es garantizar la seguridad de los sistemas tecnológicos de la librería On-line S.A. ya que al haber sido vulnerada necesita recuperar la confianza de las personas a las que les brinda el servicio. Todo esto para prevenir futuros incidentes de seguridad que puedan comprometer la información sensible de los clientes o la operatividad de la empresa mediante la evaluación detallada de la infraestructura TI. Además, se busca asegurar que la librería On-line cumpla con las normativas aplicables, ya que así la empresa puede garantizar que el servicio que ofrece, es completamente seguro y cumple los estándares requeridos para ofrecer su servicio, demostrando su compromiso en lo que respecta la seguridad de la información.

Finalmente, con los resultados de la auditoria se desarrollarán las salvaguardas y practicas pertinentes para mejorar la seguridad, como lo sería el segmentar correctamente las redes internas y fortalecer el uso de sistemas AAA.

Objetivos

Por lo tanto, para poder llevar a cabo la auditoria de forma exitosa se establecerán los objetivos puntuales sobre los que se trabajara, los cuales son los siguientes:

1. **Garantizar la seguridad de los datos personales de los clientes**: sin duda este objetivo es esencial ya que uno de los principales motivos para realizar la auditoria es que sufrió un ciberataque que comprometido las credenciales de sus clientes. Esto se logrará mediante las siguientes acciones:

- Analizando los mecanismos de autenticación y autorización para usuarios internos y externos.
- Protegiendo las credenciales almacenadas en la base de datos.

2. **Evaluar la infraestructura de red:** La seguridad de la red es un factor clave para evitar futuros accesos no autorizados, con esto se garantizará el funcionamiento correcto de el sistema, esto se logrará mediante las siguientes acciones:
    - Auditar la configuración de los firewalls y el IDS en la DMZ.
    - Verificar la correcta segmentación de la red mediante VLAN.
3. **Fortalecer las aplicaciones críticas:** La aplicación mediante la cual interactúan directamente los usuarios con la librería Online-Line es su pagina web, esta sin duda es un blanco para los ciberataques. Se buscará fortalecer la aplicación mediante las siguientes acciones:
    - Evaluar la seguridad de la aplicación web expuesta al exterior.
    - Revisar las aplicaciones internas en la intranet para identificar puntos débiles.
4. **Cumplir con las normativas aplicables:** El cumplimiento normativo es una prioridad ya que de esta forma la empresa garantizara que opera bajo los estándares legales requeridos. Se dará principal atención al Reglamento General de protección de datos (RGPD), mediante las siguientes acciones:

- Evaluar si los sistemas de la empresa cumplen con los artículos específicos del RGPD relacionados con el manejo de datos personales.

Alcance de la auditoría técnica de seguridad

El alcance de esta auditoria define los sistemas, componentes y procesos específicos que serán revisados para garantizar la seguridad de la infraestructura tecnología de la Librería On-line S.A. Por lo tanto, este aparato se centrará en detallar los limites de la auditoria, ya que se deben priorizar aquellos mas importantes de lo contrario se podrían incluir componentes que no aportan al objetivo de esta auditoría. Es así que el objetivo es abarcar solo las áreas críticas que podrían contribuir al reciente

ciberataque o que representes en un futuro un riesgo potencial afecte la seguridad del sistema y los datos personales de los clientes.

Descripción del alcance

La auditoría incluirá un análisis sobre los siguientes elementos:

- **Accesos externos VPN:** En esta parte nos enfocaremos en las conexiones seguras establecidas entre usuarios remotos y la red interna de la empresa mediante una red privada virtual. Verificando que utilice protocolos seguros, con métodos de autenticación robustos.

- **Zona DMZ: FW y IDS:** La zona desmilitarizada es una subred que separa el sistema en internos y externos, esto permite servicios públicos seguros. Auditar las reglas configuradas para evitar accesos no deseados, evaluados que tan efectivos son los IDS.

- **Publicación sitio web de la empresa:** La pagina web de la librería en donde los usuarios realizan sus compras, es muy importante auditar la seguridad de la aplicación web, con el objetivo de asegurarse de que los datos sensibles se transmitan de forma segura utilizando los protocolos adecuados.

- **Correo externo e interno:** Los correos electrónicos facilitan la comunicación tanto entre los empleados-empleados como empleados-clientes o proveedores, es importante que estén configurados adecuadamente usando cifrado (TLS/SSL) con el objetivo de proteger los correos.

- **Servicios públicos DNS y FTP:** Ambos servicios son importantes ya que mientras el DNS (convierte los nombres de dominio en direcciones IP) el servicio FTP se encarga de (transferir archivos entre sistemas). Por lo tanto, el objetivo es auditar que las configuraciones sean las adecuadas para prevenir ataques y proteger las transferencias de los archivos sensibles.

- **Infraestructura de red: router y switch:** Hay que evaluar configuraciones de seguridad, como el uso de contraseñas fuertes, la segmentación, desactivación de servicios innecesarios. Además, seria importante comprobar que estén implementadas las listas de control de acceso (ACL).

- **Aplicaciones internas Intranet y aplicaciones corporativas:** Se abarcan aquellas herramientas y plataformas que se utilizan dentro de la organización, red interna, es importante analizar vulnerabilidades en las aplicaciones que puedan ser explotadas, por aquellos agresores que logren acceder a esta red interna.

- **Zona wifi:** Es necesario auditar el uso de estándares modernos en las redes inalámbricas utilizadas por la organización para conectar dispositivos a la infraestructura de TI.

- **Segmentación en VLAN de la red interna:** servidores y usuarios: La segmentación de la red mediante VLAN organiza dispositivos en diferentes segmentos, se auditará que los servidores críticos estén aislados, para prevenir propagación de malware en caso de un acceso no autorizado.

- **Sistema AAA (autenticación, autorización y trazabilidad):** Se debe auditar que las políticas de autenticación sean adecuadas y que se registren todas las actividades relevantes para poder ser utilizadas en un análisis forense en caso de algún incidente, ya que el sistema AAA se utiliza para restringir los recursos a los que tienen acceso cada usuario, además de registrar sus actividades.

- **Sistema de antimalware:** Son todas las soluciones que fueron diseñadas para detectar, prevenir y eliminar software malicioso, es importante evaluar su afectividad, saber si esta actualizado con las ultimas firmas.

Detalle de las tareas y trabajos a realizar

En este apartado, se describirán de forma precisa las actividades específicas que se llevarán a cabo, durante la auditoria. Estas tareas están alineadas a los elementos de infraestructura, que se señalaron en el apartado anterior los cuales a su vez están alineados a los objetivos y el alcance previamente definidos.

Actividad no.1

REVISION DE LA DOCUMENTACION: La tarea consistirá en analizar toda la documentación en lo que respecta las políticas, procedimientos y configuraciones actuales de la empresa, para poder entender como esta constituida la seguridad de la empresa. Todo esto con el objetivo de identificar fallos.

Actividad no.2

EVALUACION DE LA INFRAESTRUCTURA DE LA RED: La tarea consiste en un análisis técnico sobre los dispositivos, observar la configuración que tienen y como gestionan el tráfico, hay que identificar puntos vulnerables y buscar optimizar la seguridad.

Actividad no.3

IDENTIFIACION Y ANALISIS DE LOS ACTIVOS: Nos enfocaremos en catalogar y priorizar los activos tecnológicos de la organización, hay que determinar cuáles activos son críticos para la operación y cuales requieren la atención de la auditoria.

Actividad no.4

PRUEBAS DE SEGURIDAD EN LAS APLICACIONES: Se requiere garantizar que las aplicaciones estén protegidas contra ataques comunes, esto mediante el cumplimiento de buenas prácticas de desarrollo seguro. Esto se logrará mediante herramientas como OWASP ZAP que detectan vulnerabilidades como Inyección SQL, XSS Y CSRF.

Actividad no.5

ANALISIS DE EL SISTEMA (AAA) Y EVALUACION DE SISTEMAS DE SEGURIDAD ADICIONALES: Se revisará como se gestiona el acceso a los sistemas y como se rastrean las actividades de los usuarios, verificando que la autentificación soporte métodos como “autentificación multifactor”. Por otro lado, se necesita revisaran las soluciones implementadas para detectar y mitigar amenazas, evaluando los sistemas IDS.

Actividad no.6

GENERACION DE INFORMES Y SALVAGUARDAS: Finalmente se creará un informe técnico con todos los hallazgos y acciones que deben ser corregidas, con el objetivo que de los responsables tomen decisiones basadas en el informe, el informe tendrá un plan claro para fortalecer la seguridad.

Tipos de pruebas a realizar

Para cumplir con los objetivos de la auditoria, se deben de realizar las tareas propuestas en el apartado anterior, en donde muchas de ellas nos encontramos con la necesidad de realizar pruebas para identificar vulnerabilidades y evaluar los resultados arrojados.

Es importante entender que las pruebas se pueden catalogar en 2, internas y externas, las pruebas internas evalúan la infraestructura interna de la organización, mientras que las pruebas externas se centrar en vectores que provienen del exterior. De esta forma las pruebas que se llevarán a cabo serán las siguientes:

1. Pruebas de penetración: Esta prueba estará centrada en utilizar la herramienta OWASP ZAP, que se encargará de simular un ataque desde el exterior para identificar vulnerabilidades. Será catalogada como externa, ya que se centra en ataca la aplicación desde fuera de la empresa.

2. Análisis de vulnerabilidades: Se realizarán pruebas con herramientas como Nessus, con el objetivo de encontrar alguna vulnerabilidad en servidores y dispositivos de red. Esta prueba será catalogada como interna debido a que será realizada en sistemas internos.

3. Revisión de configuraciones: Se validarán las configuraciones de firewalls, VPN y IDS, esto se debe a que deben estar configurados correctamente para evitar ser explotados, las pruebas se llevaran acabo de la siguiente forma:

    - Pruebas en firewalls: Se revisará que las reglas permitan solo el trafico necesario dentro de la red interna, permitiendo únicamente el trafico HTTP/HTTP entre los usuarios internos y el servidor web.
    - Redes Privadas Virtuales (VPN): Se debe verificar que los usuarios internos se autentiquen mediante contraseñas seguras, de igual forma se realizaran pruebas de cifrado, para confirmar que se utilizar protocolos seguros.
    - Sistemas de Detección de Intrusos (IDS): Se hará una prueba generando tráfico sospechoso dentro de la red, como lo sería el escaneo de puertos, con el objetivo de verificar si el IDS los detecta y genera alertas. Además de revisar si las alertas están configuradas adecuadamente.

Identificar las limitaciones aplicables

Este apartado se enfoca en identificar posibles restricciones o limitaciones que podrían afectar el desarrollo de la auditoria, por lo tanto, se formara un listado de aquellas que el equipo de auditoria considera que puedan tener una alta probabilidad.

1. Restricción de tiempo: La auditoria se ve limitada por el tiempo disponible que se tendrá para realizar la misma, considerando el plazo máximo, algunas pruebas pueden verse afectadas por factores externos.

2. Restricción a la infraestructura interna: El acceso a ciertos sistemas podría generar un problema, ya que la empresa podría contar con políticas que restrinjan su acceso a los mismo.

3. Presupuesto limitado: Es importante destacar que la auditoria se vera sujeta a los recursos financieros asignados por la Librería On-line S.A. por lo que el plan de auditoria aun tiene que pasar por diferentes áreas que señalen si el plan completo se lleva a cabo o se reduce.

4. Empresas externas: La empresa destaca que en los procesos de pagos depende de la colaboración de un proveedor externo, por lo que ciertas pruebas se verán afectadas por las restricciones de la empresa externa.

Metodologías.

Las metodologías desempeñan un papel fundamental en una auditoria técnica de seguridad, ya que proporcionan un enfoque estructurado además de que ayuda a estandarizar la forma de evaluar la seguridad de los sistemas, junto con la identificación de vulnerabilidades.

Por ejemplo, las metodologías como OWASP, NIST CSF O ISO/IEC27001, fueron desarrolladas y validadas por expertos, estableciéndose como un marco común ya que estas metodologías permiten evaluar la seguridad bajo criterios en común. Entonces podemos concluir que la importancia radica en que los marcos facilitan la comparación de los resultados entre auditorias realizadas en diferentes organizaciones y garantizan que los análisis cubran los aspectos relevantes, evitando omisiones críticas.

Por lo tanto para poder llevar acabo exitosamente la auditoria de la empresa librería On-line S.A. se opta por utilizar las siguientes metodologías:

1. OWASP Testing guide: esta metodología proporciona una forma estructurada de evaluar la seguridad de aplicaciones web. Se enfoca en identificar vulnerabilidades específicas como inyección SQL, cross-site scripting y controles de acceso deficientes.
2. NIST Cybersecurity Framework (CSF): Este es un marco de trabajo que nos proporciona una forma de gestionar la ciberseguridad de la empresa, analizando el sistema de gestión actual de la empresa con lo que se requiere basándose en los puntos de la empresa, además de que el marco se ajusta a cualquier tipo de empresa lo que la hace idónea para poder realizar exitosamente nuestra auditoria.
3. ISO/IEC 27001: Este estándar ayuda a establecer los requisitos para implementar un sistema de gestión de seguridad de la información, se utiliza para garantizar el cumplimiento de normativas. Se enfoca en revisar las

políticas y procedimientos de seguridad de la organización con el objetivo de asegurar que estén alineados con los requisitos de ISO 27001. Además, nos ayudara a identificar ares de incumplimiento y proponer medidas correctivas.

La combinación de estas metodologías nos permitirá abordar la auditoria desde un enfoque más alineado en lo que respecta el análisis técnico, cumplimiento normativo y mejorar la gestión de la seguridad.

Planificación:

Este apartado establece un cronograma detallado para realizar la auditoria, nos enfocaremos en dividir el trabajo que se realizara previamente detallado en la sección de tareas, en plazos. Lo que reflejara una ejecución ordenada.

Tarea 1: REVISION DE LA DOCUMENTACION.

Duración: 3 días.

Tarea 2: EVALUACION DE LA INFRAESTRUCTURA DE LA RED:

Duración: 4 días.

Tarea 3: IDENTIFIACION Y ANALISIS DE LOS ACTIVOS:

Duración: 2 días.

Tarea 4: PRUEBAS DE SEGURIDAD EN LAS APLICACIONES:

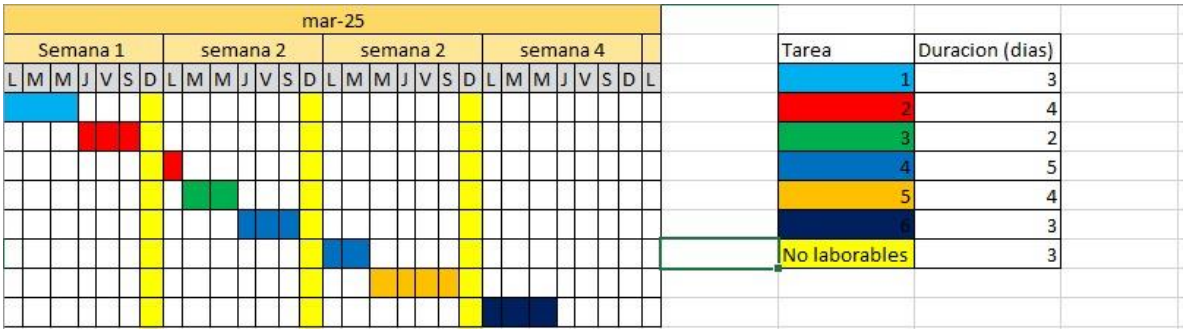
Duración: 5 días.

Tarea 5: ANALISIS DE EL SISTEMA (AAA) Y EVALUACION DE SISTEMAS DE SEGURIDAD ADICIONALES:

Duración: 4 días.

Tarea 6: GENERACION DE INFORMES Y SALVAGUARDAS:

Duración: 3 días.



Recursos necesarios

Tipo de recurso	Recurso
Recursos hardware	- Laptop o estación de trabajo - switch - router auxiliar - Almacenamiento externo
Recursos software	- Nessus - OWASP ZAP - Nikto - Wireshark - Nmap - Microsoft Office
Recursos Humanos	- Auditor líder - Especialista en aplicaciones web - Analista de redes - Especialista en normativas y cumplimiento - Asistente técnico

Entregables

Informe técnico detallado:

Este entregable contendrá el análisis técnico completo de la auditoria, es decir todos los hallazgos obtenidos, incluirá una descripción detallada de las vulnerabilidades detectadas en todos los sistemas. También se presentará un análisis de impacto de las vulnerabilidades que se hayan registrado y las posibles formas en que podrían ser explotadas por atacantes. Para poder complementar esto se expondrán datos obtenidos mediante las diferentes herramientas de auditoría.

Resumen ejecutivo

Este informe tendrá un resumen de los resultamos mas importantes para ser presentados de forma comprensible a los directivos y responsables de la toma de decisiones. Resaltara las vulnerabilidades críticas que podrían afectar a la organización. También incluirá recomendaciones estratégicas con una escala de prioridad para que se pueda observar cuales deben de ser atacadas de inmediato. El resumen será redactado en un lenguaje comprensible sin términos técnicos complejos, ya que se enfoca en explicar los problemas desde una perspectiva sobre como la empresa abordará la ciberseguridad en términos simples.

Matriz de riesgos

Este entregable se enfoca en clasificar los riesgos en un formato tabular, claro y practico.

Sera categorizado según los siguientes puntos.

-Criticidad

-Probabilidad

-Impacto

Lo mas importante es que incluirá una columna con recomendaciones especificas para mitigar cada riesgo y un campo que asigna prioridades para facilitar la implementación de correctivas.

Procedimientos de comunicación con los responsables de proyecto.

La comunicación que se implementará para mantener informados de forma adecuada a los responsables será llevada mediante.

1. REUNION INICAL: se organizará una reunión de inicio para validar el alcance, objetivos y prioridades y que los responsables estén de acuerdo con ellos.
2. INFORMES DE PROGESO: se enviarán reportes semanales que incluirán el avance de las tareas y hallazgos preliminares y cualquier desviación con respecto al cronograma
3. COMUNICACIÓN INMEDIATA: en caso de identificar riesgos severos, se notificará de inmediato a los responsables para implementar las medidas necesarias.

Metodología SCRUM:

1. Sprint semanales: se deben organizar tares de la auditoria en ciclos cortos, revisando los avances.
2. Daily Satandups: las reuniones diarias serán enfocarán en sincronizar al equipo sobre las tareas realizadas, los pendientes y los posibles impedimentos.
3. Revisión y retrospectiva: Al final de cada sprint, se realizará una revisión de los resultados obtenidos.

Anexo I: Acuerdo de autorización

Fecha: 27/01/2025

Empresa: Librería On-Line S.A.

Responsable: Juan Aristeo

Auditor: InfoSecurity

Por medio de este documento, la Librería On-line S.A. autoriza formalmente la realización de una auditoria técnica de seguridad sobre la infraestructura tecnológica. Este acuerdo establece los términos y condiciones bajo los cuales se llevará acabo la auditoria, así como los limites y responsabilidades de ambas partes.

El propósito de este documento es garantizar que las actividades de la auditoria sean realizadas de manera transparente y bajo los términos establecidos, con el fin de identificar las vulnerabilidades en los sistemas de TI de la Librería On-Line S.A.

CLAUSULAS

PRIMERA: Las actividades que se realizaran como parte de esta auditoria incluyen, pero no se limitan a:

- Pruebas de penetración en la aplicación web pública.
- Revisión de configuraciones de dispositivos de red, como firewalls, router y VPN.
- Análisis de vulnerabilidades en servidores, bases de datos y sistemas de autenticación.
- Evaluación de cumplimiento con normativas como el RGPD

Limites:

No se autoriza realizar pruebas destructivas que puedan interrumpir los servicios de la organización o comprometer la integridad de los datos.

SEGUNDA: El auditor se compromete a:

- Realizar todas las actividades con la máxima ética y profesionalismo
- Garantizar la confidencialidad de la información obtenida durante la auditoria.
- No divulgar ningún dato relacionado con la empresa sin el consentimiento explícito de la Librería On-line S.A.

TERCERA: La librería On-Line S.A. se compromete a:

- Proporcionar acceso a la documentación, sistemas y recursos necesarios para la auditoria.
- Designar a un responsable interno para facilitar la comunicación y la coordinación de las actividades.
- Responder oportunamente las solicitudes de información.

QUINTA: Toda la información obtenida durante la auditoria será considerada confidencial y será manejada exclusivamente para los fines establecidos en este acuerdo.

FIRMA DE ACEPTACION

Librería On-Line S.A.	InforSecurity