LA UNIVERSIDAD EN INTERNET

Infosecurity

Auditoria de Seguridad

Librería On-Line S.A.

GRUPO 29

Presentado por:

Blanca Paola Toledo Martínez

Angel Ramón Paz López

Braulio David Velasco Castillo

LA UNIVERSIDAD EN INTERNET

Asignatura	Datos del alumno	Fecha
Auditoría de seguridad	Apellidos: Grupo	31/01/2022
	Nombre: 29	

Actividad grupal: Plan de auditoría técnica de seguridad

Índice

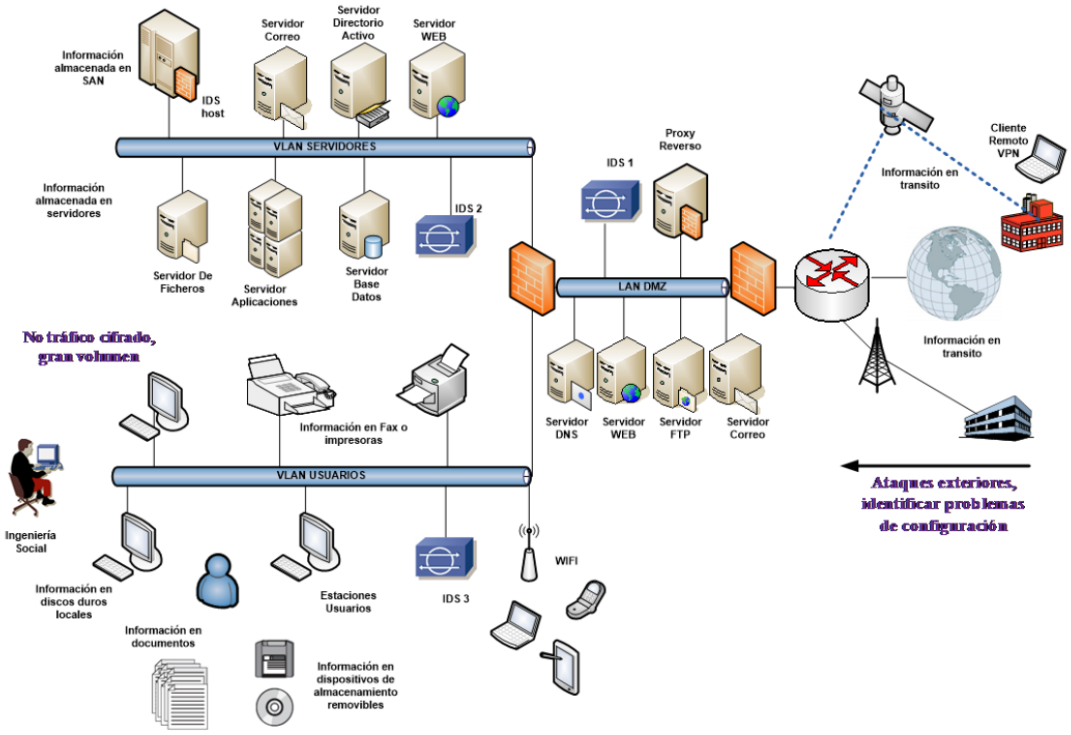
Introducción.

Reflexiono que dentro de una actividad tan reciente y expansiva como la auditoria, es importante mencionar que el muestreo siempre ha sido parte importante en su desarrollo, haciendo de ella una evaluación de la eficiencia y eficacia que tiene una organización, identificando los errores y con ello plantear las correcciones correspondientes, siendo indispensable la evaluación y la revisión de los sistemas de cómputo, por medio de diversos procesos que permitan identificar las fallas que pueda tener la organización para una mejor toma de decisiones.

En el presente manuscrito de plan de auditoría, realizara un estudio detallado sobre la compañía y todos los elementos de los sistemas de TI, todo esto para poder determinar las prevenciones de seguridad para que los usuarios puedan realizar sus adquisiciones en línea y que este proceso pueda proveer de credibilidad, honestidad y disponibilidad de operaciones efectuadas por medio del sitio web de la **Librería Online S.A.**

Propósito de la auditoría.

Lo primordial de este manuscrito es establecer si la organización cumple con la legislación de seguridad, identificando las debilidades y deficiencias de la arquitectura de red, de acuerdo con la figura 1, y de esta manera poder concluir cuales los niveles de riesgo en la arquitectura de red de la **Librería Online S.A.** y poder determinar de qué manera mitigarlos o eliminarlos.



Objetivos de la auditoría.

- Comprobar e identificar cuáles son los riesgos a los que está expuesto el sitio web de la **Librería Online S.A.**, referente a las transacciones con los clientes.
- Evaluar la administración de los dispositivos de almacenamiento básico del área de informática.
- Valorar los procedimientos de control de operación, analizando su estandarización y evaluar su cumplimiento.
- Establecer un plan para asegurar una mayor integridad, confidencialidad y confiabilidad de la información para la continuidad del negocio a mediano y largo plazo.

Alcance de la auditoría técnica de seguridad (identificar las limitaciones).

Los problemas de seguridad que ha tenido la **Librería Online S.A.**, han impactado en la adquisición de sus productos, poniendo en juego la perseverancia del negocio, ya que ha sido un factor importante en la confianza de sus clientes para poder utilizarla.

Fase I. Estudio Inicial.

La principal acción con el plan propuesto es identificar los riesgos de exposición, además establecer mediante una metodología de auditoría y tener una mayor seguridad.

- Estructura organizacional del área de TI de la **Librería Online S.A.**
- Servicios informáticos relacionados a TI.
- Aplicaciones informáticas
- Organigrama
- Departamentos
- Flujos de información
- Puestos de trabajo

Fase II. Entorno Operacional.

La principal acción es realizar un análisis del funcionamiento de la **Librería Online S.A.**, y de los mecanismos tecnológicos como lo son el hardware y el software.

- Verificación de la arquitectura y diseño de las aplicaciones en el entorno empresarial.
- Estado del Centro de Procesamiento de Datos en la Nube, el modo del funcionamiento y responsables.
- Revisión de las Políticas de Seguridad de la Información.
- Verificación de Perfiles y funciones, así como la revisión de Procesos y Procedimientos.
- Auditoria a la Base de Datos, tamaño, número de accesos y actualización.

Todo esto para lograr de una manera competente en un corto tiempo readquirir la confianza de los clientes, y de esta manera restaurar la continuidad del negocio a mediano y largo plazo.

Metodologías que se utilizarán.

La auditoría se llevará a cabo sobre los sistemas de TI de la **Librería Online S.A.**, donde la principal prioridad es la seguridad de la tienda web, basándonos en las normas internacionales ISO/IEC 27001:2013, seleccionando una metodología para el análisis y gestión de riesgos MAGERIT, que nos servirá para concienciar de la existencia de riesgos y su importante necesidad de gestionarlos, seleccionando solamente los dominios relacionados solamente con en el aspecto tecnológico.

- A5 Políticas de la Seguridad de la información.
    - Proporcionando orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.
- A6 Organización de la Seguridad de la información.
    - En la organización interna es importante establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
    - Dispositivos móviles y teletrabajo, para poder garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
- A9 Control de acceso.
    - Requisitos de negocio para el control de acceso, limitando el acceso a la información y a las instalaciones de procesamiento de información.
    - Gestión del acceso de usuarios, asegurando el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.
    - Responsabilidades del usuario, haciéndolos responsables de salvaguardar su información de autenticación.
    - Responsabilidades del usuario, Impedir el acceso no autorizado a los sistemas y aplicaciones.
- A11 Seguridad Física y del Entorno.
    - Áreas seguras, evitando accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información de la organización.
    - Equipamiento, previniendo perdidas, daños, hurtos o comprometer los activos, así como la interrupción de las actividades de la organización.
- A13 Seguridad en las telecomunicaciones
    - Gestión de la seguridad de red, asegurando la protección de la información en redes y la protección de la infraestructura de soporte.

- Intercambio de información, mantener la seguridad de la información intercambiada dentro de una organización y con cualquier otra entidad.

Plan de recolección y análisis de datos (incluir las herramientas a utilizar).

Para el desarrollo y análisis de la información de **Librería Online S.A.** se recurrirá a los siguientes mecanismos de recolección:

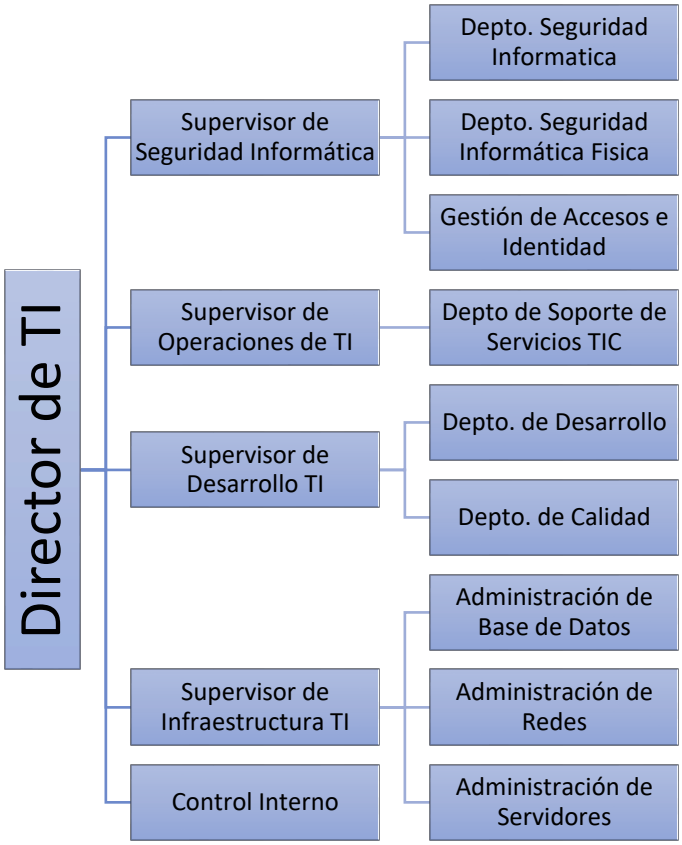
- Entrevistas
- Cuestionarios
- Consultas
- Reuniones
- Observación
- Revisión de la documentación
- Indagación
- Comparación

Para el procesamiento de la información obtenida de **Librería Online S.A** se utilizará el siguiente criterio:

- Levantamiento de Información
- Clasificación de la información obtenida
- Registro de la información
- Análisis de información
- Verificación de la información
- Archivo de la información

Organización y recursos necesarios.

Se logra establecer los recursos humanos y materiales que se demandan para la realización de la auditoria. En la figura 1.1 se describe el organigrama con la jerarquía y las diferentes áreas de TI que estarán involucradas.



Los recursos que se utilizaran en la auditoria constan de un equipo de 3 auditores, los cuales poseen las herramientas necesarias para el desarrollo de esta, los cuales estarán en constante comunicación con los responsables de cada

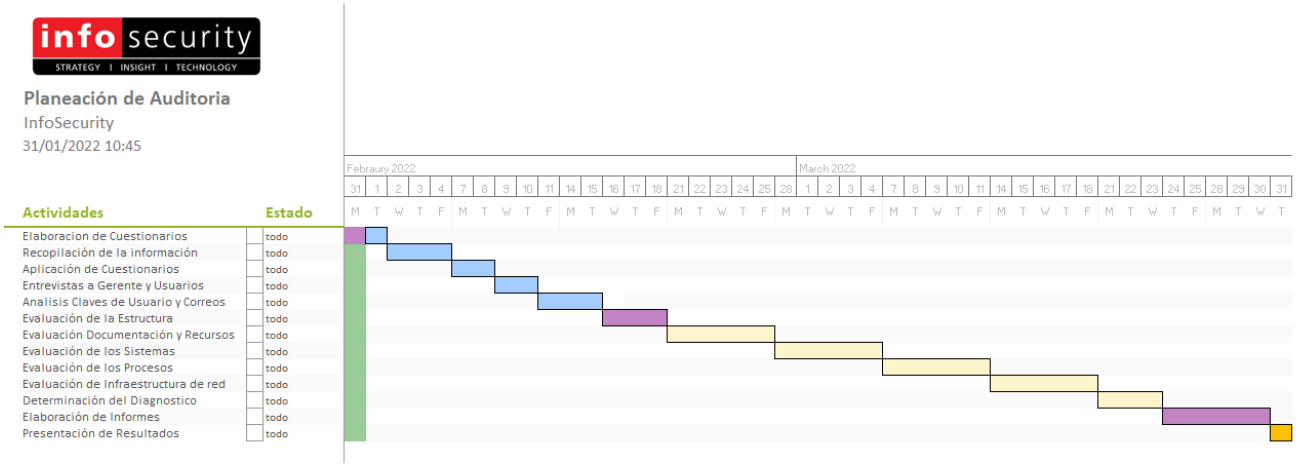
Plan de comunicación.

La comunicación que se establece durante el periodo de auditoria es la siguiente:

- Los jueves se establecerá una minuta de 50 min para informar a la dirección e involucrados el avance de la auditoria.
- El canal de comunicación se establecerá directamente con los representantes de **Librería Online S.A.,** áreas involucradas y la empresa Auditora.
- En caso de que se anexen solicitudes derivadas de las reuniones, entrevistas, cuestionarios, etc. Se tendrá una reunión a todos los involucrados con las fechas compromiso y responsables.

Planificación.

Con el fin de poder efectuar las actividades se propone el siguiente calendario de actividades teniendo en cuenta que se llevara a cabo la auditoria en los días hábiles.



Entregables de Auditoria

CICLO	INFORMES
Planificación	Diseño de la Planificación de trabajo con sus respectivas actividades
Ejecución	Informe de avance de la auditoria
Comunicación de Resultados	Informe preliminar de la auditoria con su respectivo informe de supervisión.
	Informe final por cada uno de los procesos auditados.
	Entrega de toda la documentación los cuales serán entregados en forma física y medio electrónico con las medidas de seguridad pertinentes.

Evaluación de Riesgos

Es relacionar las amenazas con las vulnerabilidades en relación con la capacidad de respuestas y autogestión que pueda tener una organización para así determinar su importancia.

Amenaza	Impacto	Probabilidad	Riesgo
Ransomware	Catastrófico	Posible	Alto
Robo de Credenciales	Mayores	Posible	Alto
Infección por Spyware	Mayores	Muy Probable	Alto
Inyección SQL	Mayores	Posible	Alto
Malware	Moderado	Muy Probable	Medio
Ataques DDoS	Mayores	Posible	Alto
Ataques XSS	Mayores	Probable	Alto
Intrusos	Mayores	Posible	Medio
Acceso a la red por personal no autorizado	Mayores	Posible	Alto
Fallo en servicios de comunicación	Menor	Poco probable	Bajo
Fallo en equipos de red	Menor	Poco probable	Bajo
Incumplimientos contractuales por parte de los clientes	Menor	Posible	Bajo
Acceso a sistemas por personal no autorizado	Mayores	Posible	Alto

Anexo A: Acuerdo de Autorización.

LAS PARTES

Las partes de este Acuerdo son la tienda de libros en línea "Librería On-Line S.A." y la empresa InfoSecurity.

ARTICULO 1.- ÁMBITO DE APLICACIÓN Y OBJETIVOS DEL ACUERDO

El principal objetivo de la cooperación bilateral es la ejecución de actividades de auditoria para analizar todos los sistemas de tecnologías de la información (TI) de Librería On-Line y de implementar salvaguardas en función de los hallazgos y del nivel de riesgo con el objetivo de recuperar y mantener la actual posición en el mercado de su venta electrónica de libros.

ARTÍCULO 2.- L A CONTRIBUCION

Tienda de libros en línea "Librería On-Line S.A." deberá poner a disposición la cantidad que no exceda en dólares la cantidad de Siete Mil ($ 7.000) para la aplicación del examen y la investigación de campo.

Los fondos serán desembolsados a InfoSecurity.

ARTÍCULO 3.- COMPROMISOS DE LA EMPRESA INFOSECURITY

INFOSECURITY se compromete:

1) Que será responsable de la aplicación de la revisión e investigación de campo, de acuerdo con la propuesta de fecha 31 de enero 2022,
2) Planificar, organizar, realizar y el seguimiento de la revisión y trabajo de campo.
3) Proporcionar informes profesionales, administrativos y físicos y apoyo logístico necesarios para la implementación exitosa de la revisión y la investigación de campo.
4) Que la gestión y el control interno de recursos relacionados con el examen y la investigación de campo están adecuadamente manejados.

ARTÍCULO 4.- PLANIFICACIÓN, REVISIÓN, INFORMACIÓN Y EVALUACIÓN

La tienda de libros en línea "Librería On-Line S.A." y la empresa InfoSecurity se reunirán, si es necesario, para dar seguimiento a los avances de la revisión y la investigación de campo. Las reuniones serán solicitadas por cualquiera de las partes, cuando sea necesario. A la expiración del período de actividad la empresa InfoSecuritu presentará a la tienda de libros en línea "Librería On-Line S.A." un Informe de Resultados. Los informes serán sometidos a la tienda de libros en línea "Librería On-

Line S.A.” a más tardar el 28 de febrero del 2022. Los informes resumirán los resultados obtenidos y esperados y contendrán un análisis de cualquier desviación o problemas de ese hecho. Además del Informe de Resultados, InfoSecurity presentará a la tienda de libros en línea “Librería On-Line S.A.” un informe preliminar y un informe final sobre la revisión, de acuerdo con los objetivos esperados indicados en la propuesta presentada por InfoSecurity a tienda de libros en línea “Librería On-Line S.A.”

Febrero 25, 2022. El informe preliminar será presentado a tienda de libros en línea “Librería On-Line S.A.” inmediatamente después del examen de la fase I del estudio, y el informe final sobre el examen se presentarán a más tardar el 31 de marzo 2022. La empresa InfoSecurity informará sin demora a la tienda de libros en línea “Librería On-Line S.A.” si los informes y los planes no pueden ser presentados según lo acordado. Con independencia de las rutinas aprobadas para los informes, las partes informarán sin demora a los demás, si surge una situación que hace probable que el examen y la investigación de campo no se llevarán a cabo según lo acordado. InfoSecurity presentará a la tienda de libros en línea “Librería On-Line S.A.” con cualquier otra información relativa a la revisión y la investigación de campo que la tienda de libros en línea “Librería On-Line S.A.” considere razonablemente necesario y se permita a los representantes de la tienda de libros en línea “Librería On-Line S.A.” visitar los lugares de la empresa InfoSecurity e inspeccionar la propiedad, bienes, registros y documentos relacionados con la revisión y la investigación de campo. La empresa InfoSecurity cooperará con tienda de libros en línea “Librería On-Line S.A.” y ayudar en la realización de actividades de seguimiento y evaluación del impacto de la revisión y la investigación de campo.

ARTÍCULO 5.- TERMINACION

El presente Acuerdo será válido hasta el 31 de marzo 2022 salvo que se resuelva antes de seis meses, mediante una notificación escrita por cualquiera de las Partes, En caso de incumplimiento grave del Acuerdo, la tienda de libros en línea “Librería On-Line S.A.” puede rescindir el contrato con efecto inmediato. En el caso de terminación por la tienda de libros en línea “Librería On-Line S.A.”, la terminación no se aplicará a los fondos irrevocablemente comprometidos de buena fe por la empresa InfoSecurity a terceros antes de la fecha de la notificación de terminación, siempre que los compromisos se realizaron de conformidad con el presente Acuerdo. En el caso de terminación por InfoSecurity, ningún fondo se pondrá a disposición para las actividades después de la expiración del presente Acuerdo.

ARTÍCULO 6.- FECHA EFECTIVA

El presente Acuerdo entrará en vigor en la fecha en que ambas partes han firmado. Dos originales del presente Acuerdo, se han firmado, de los cuales las partes han tenido una cada uno.

Tegucigalpa, MDC 31 de enero, 2022

Tienda de Libros "Librería On-Line S.A.",	Empresa InfoSecurity
_____	_____
Firma	Firma
Jan Robberts Miguel Ángel Mejía	Roberto Carlos Larach
Gerente	Presidente

Anexo B: Acuerdo de Confidencialidad.

Nosotros la empresa InfoSecurity en desarrollo del rol de Auditores Técnicos de Seguridad, entendemos que la labor que desempeñaremos se tendrá acceso a información, escrita, oral, digital o de cualquier otra forma relacionada con la actividad de auditoría a cargo de la Oficina de Control Interno ya sea planes, listas de chequeo, registros, aplicaciones, informes, documentos, entrevistas, etc. Teniendo en cuenta lo anterior, manifestamos que nos comprometemos a:

1) Mantener reserva y confidencialidad de la información antes descrita, no divulgarla por ningún medio, no transmitirla o compartirla a cualquier persona que no sea miembro del equipo de InfoSecurity.
2) No usar la información tanto directo como indirectamente en beneficio personal o de terceros, la información recopilada solo se podrá utilizar para cumplir las actividades de la auditoria técnica.
3) No enviar archivos que contengan información que este relacionada a las actividades de la auditoria a través de correos electrónicos u otros medios a los que tenga acceso, a personal que no sea del equipo de trabajo de auditoría.

Asimismo, nos comprometemos a cumplir con las normas y políticas de seguridad de la tienda de libros en línea “Librería On-Line S.A.”, la normativa técnica y administrativa establecida por la Oficina de control Interno para el desarrollo de auditorías y todas aquellas directrices que regulen el desempeño profesional de las actividades que se desarrollaran en la tienda de libros en línea “Librería On-Line S.A.”, así como las leyes y regulaciones relevantes de Mexico. En caso de tener dudas sobre lo que está o no permitido divulgar conforme a este Compromiso de Confidencialidad nos comprometemos a consultar al Líder de Auditoría. En caso de incumplimiento de lo establecido en el presente documento, la Oficina de Control Interno lo comunicará a las instancias competentes con el fin que inicien las actuaciones pertinentes. Dejamos expresa constancia que este Compromiso de Confidencialidad lo he suscrito a los 31 días de enero del año 2022.

CC Librería On-Line S.A.
CC InfoSecurity

Hoja de control de actividad grupal

Cada integrante debe llenar e incluir al final de su documento el siguiente registro.

Hoja de control de actividad grupal			
	Marcar con una **X** lo que proceda		
Asistencia a reuniones de equipo	Asistencia a una sesión o ninguna	Asistencia a dos sesiones	Asistencia a tres sesiones
Angel Ramón Paz López			x
Braulio David Velasco Castillo			x
Blanca Paola Toledo Martínez			x
Tareas o entregas a realizadas	Ninguna o una tarea	Dos tareas	Tres tareas
Angel Ramón Paz López			x
Braulio David Velasco Castillo			x
Blanca Paola Toledo Martínez			x