

Asignatura	Datos del alumno	Fecha
Auditoría de seguridad	Apellidos: Paz López	10/01/2022
	Nombre: Angel Ramón	

ANTECEDENTES

La Empresa Viento en popa es una empresa que se dedica a planificar actividades náuticas, impartir clases de navegación ofreciendo la certificación de Patrón de Embarcaciones de Recreo (PER), la empresa cuenta con una plataforma web como canal de información y venta para que sus clientes naveguen en ella y brindar cualquier servicio que ellos necesiten, cabe mencionar que dicha plataforma web está basado en tecnología Java. La empresa posee 500 empleados distribuidos incluyendo su centro de procesamiento de datos y sus principales sucursales en las 3 principales ciudades del país.

Estructura Organizacional asociada a la página web

Rol	Interacción	Tareas
Administración	Web, aplicación móvil	Seguimiento de cobros, seguimiento de clientes para su respectiva certificación, seguimiento inventario, historial de clientes, actualizar catálogo de productos, precios, promociones y paquetes
Clientes	Web, aplicación móvil	Consulta de pagos, cursos, consulta de productos, pagos, impresión de facturas, soporte técnico, compras
Ventas	Web, aplicación móvil	Seguimiento inventario, catálogo de productos, historial de clientes
Académica	Web, aplicación móvil	Catálogo de cursos, seguimiento de cliente para su certificación

Soporte TIC	Web, aplicación móvil, Servidor	Soporte página Web, soporte a Clientes, Soporte Base de Datos, Control de Usuarios
Soporte al Cliente	Web, aplicación móvil,	Atender las solicitudes de dudas, reclamos, quejas de los clientes

La Empresa Viento en Popa cuenta con controles generales en relación a la ISO (27002, 2017) con el que cuenta con 5 controles activos.

Referencia	Control	Nivel de Cumplimiento	Madurez
6.1.1	Asignación de responsabilidades para el seguimiento de la información.	70%	Definido
9.1.1	Políticas de Control de Accesos	50%	Definido
9.3.1	Uso de información confidencial para la autenticación.	50%	Definido
9.4.1	Restricción del acceso a la información.	40%	Definido
12.1.1	Documentación de procedimientos de operación	40%	Definido
12.4.1	Registro y gestión de eventos de actividad.	0%	No existe, será implementado
12.7.1	Controles de auditoría de los sistemas de información	0%	No existe, será implementado
13.2.4	Acuerdos de confidencialidad y secreto.	0%	No existe, será implementado
16.1.1	Responsabilidades y procedimientos	0%	No existe, será implementado
18.1.4	Protección de datos y privacidad de la información personal.	0%	No existe, será implementado

PRESENTACIÓN DE RIESGOS INHERENTES AL PORTAL WEB

La web de viento en popa está basada en tecnología Java el cual, así como las demás tecnologías esta propenso a ciberataques, el cual listamos los riesgos inherentes del servicio web. Las valoraciones tanto como el top de vulnerabilidades se toman como referencia de la metodología OWASP (OWASP, 2017)

Riesgo	Vulnerabilidad	Explotabilidad	Prevalencia	Detección	Impacto técnico	Impacto de negocio	Puntaje
Pérdida de datos, corrupción o divulgación	A1:2017 Inyección	3.Facil	2.Comun	3.Facil	3.Grave	Grave	8.0
Acceso a personas no autorizadas	A2:2017 Perdida de Autenticación	3.Facil	2.Comun	2.Comun	3. Grave	Grave	7.0
Robo de Información	A3: 2017 Exposición de datos	2. Promedio	3. Difundido	2. Promedio	3.Grave	Grave	7.0
Divulgación de información no autorizada, la modificación o destrucción de todos los datos	A5:2017 Pérdida de Control de Acceso	2.Promedio	2.Comun	2.Promedio	3.Grave	Grave	6.0
Vulneración completa del del sistema.	A6:2017 Configuración de Seguridad Incorrecta	3.Facil	3.Difundido	3.Facil	2.Moderado	Moderado	6.0
Aplicaciones y APIs serán vulnerables	A8:2017 Deserialización Insegura	1.Dificil	2.Comun	2.Promedio	3.Grave	Grave	5.0
Fuga de información, fallos no registrados	A10:2017 Registro y Monitoreo Insuficientes	2.Promedio	3.Difundido	1.Dificil	2.Moderado	Moderado	4.0

PLAN DE AUDITORIA


Objetivo

El objetivo principal de la auditoria es identificar y describir los riesgos y las vulnerabilidades que pudiesen suscitarse en la plataforma web de la empresa Viento en Popa por lo cual se creara un plan de acción tanto preventivo como correctivo para poder mitigar cualquier actividad anómala que se presente, detallando los pasos de auditoría necesarios y desglosando el trabajo planificado en un cronograma. Se entregará un programa de trabajo y un plan de Comunicación acotado en 2 meses para el diseño y puesta en marcha de la auditoria y la entrega de los resultados de ello definidos la cual se incluirán en el informe solicitado.

Alcance

El alcance establecido para Viento en Popa se sitúa en todas las áreas organizativas de los cuales tengan relación directa con el sitio web con la necesidad de realizar y proporcionar hallazgos y las respectivas recomendaciones con el objetivo de identificar los riesgos del sitio web, para ello se auditaron los controles de seguridad asociados a los riegos inherentes del portal.

Calendario de Actividades

		Periodo en ejecución								Responsable
		Mes 1				Mes 2				
Nº	Actividad	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	
1	Conformacion del Equipo de Auditoria									Oficina de Auditoria
2	Elaboracion del plan de Auditoria									Oficina de Auditoria
3	Planeacion inicial de la Auditoria									Oficina de Auditoria
4	Confirmacion de objetivos y alcances									Oficina de Auditoria, Viento en Popa
5	Desarrollo y Auditoria									Viento en popa
6	Recopilacion y Analisis de Resultados									Oficina de Auditoria
7	Presentacion de Resultados									Oficina de Auditoria

Recursos

El equipo de auditoría de seguridad para el portal web de Viento en popa consta de un equipo profesional de 1 Auditor Líder y 2 Auditores más con horarios asociados a la operación de la

compañía, el cual poseen los conocimientos necesarios y las herramientas para realizar las actividades de auditoría de manera eficaz y eficiente.

Metodología

La metodología que se utilizará para la ejecución de la auditoría de seguridad de la plataforma web de la empresa Viento en Popa será OWASP que es una metodología orientada a orientada al análisis de seguridad de aplicaciones Web y a prestar servicios orientados al análisis y evaluación de riesgos de la web, basándonos en el top 10 de vulnerabilidades (OWASP, 2017).

Plan de Comunicación

Las actividades que se realizarán durante el periodo de auditoría del sitio web Viento en Popa se reflejarán en un plan de comunicación para organizar los procesos de comunicación y realizar un trabajo comunicativo para así facilitar la orientación y llevar al día todas las actividades que se necesitan realizar y promover el seguimiento y evaluación de los procesos.

1. Cada 15 días se realizará reunión con la dirección general de la empresa viento en Popa para el avance de la auditoría.
2. Se realizarán encuestas a los usuarios inscritos en los cursos de la página los días 5 de cada mes durante el tiempo de auditoría (2 meses).
3. Análisis de los resultados de las encuestas el cual debe estar listo y presentada a la dirección general en las respectivas reuniones.
4. El canal de comunicación se realizará directamente entre el representante de Viento en Popa y la Oficina Auditora.
5. Informe Final se realizará en la reunión de cierre del proceso de auditoría.

Entrega de Resultados

- Informe preliminar el cual tiene que ser entregado a la dirección general de la empresa y a todos los interesados.
- Informe final entregado a la dirección general, al área auditada en el momento que se realice la reunión de cierre del proceso de auditoría

Desarrollo

Se utilizará la metodología del análisis de riesgos basada en el estándar ISO 27002 en la cual se identificarán los riesgos potenciales que afecten al sitio web, se identificara también la calidad, eficacia y eficiencia de los controles implementados mediante la ejecución de pruebas sustantivas en todas las actividades técnicas, normativas y de cumplimiento. Las pruebas sustantivas que se realizaron son de acuerdo al Top 10 de las vulnerabilidades (OWASP, 2017) :

- Inyección de Código SQL y XML
- Monitoreo de los servicios web y logs del sistema
- Prueba en el acceso y autenticación del portal web tanto para clientes, administradores y demás usuarios.

Hallazgos, riesgos asociados y controles propuestos identificados para cubrir cualquier deficiencia en la plataforma web.

Descripción	Activo en Riesgo	Riesgo Owasp	Valor	Control ISO 27002	Medidas
La aplicación utiliza datos que no son confiables en la Construcción de varios comandos SQL vulnerable que se utilizan en la aplicación	Todas las Bases de datos.	A1:2017	8	Ninguno	Se requiere separar los datos de los comandos y las consultas.
El tiempo de vida de las sesiones de la aplicación no están configurados correctamente	Todas las Bases de datos.	A2:2017	7	ISO 9.3, 9.4	Utilizar un gestor de sesión en el servidor, integrado y que sea seguro que genere ID de sesión aleatorio nuevo, este no debe incluirse en la URL, debe almacenarse de forma segura y ser invalidado después del

					cierre de sesión o de un tiempo de inactividad determinado. .
Se utilizan hashes simples para almacenar las contraseñas de los usuarios.	Todas las Bases de datos.	A3:2017	7	Ninguno	Almacenar las contraseñas utilizando funciones de hashing adaptables, además usar hashes con SALT, como Argon2, scrypt, bcrypt o PBKDF2.
La aplicación utiliza datos no validados en una llamada SQL para acceder a información de cualquier cuenta	Todas las Bases de datos.	A5:2017	6	ISO 9.1, al 9.4	Los desarrolladores deben incluir pruebas de control de acceso en sus pruebas unitarias y de integración.
Un proveedor de servicios en la nube (CSP) por defecto permite a otros usuarios del CSP acceder a sus archivos desde Internet	Todas las Bases de datos.	A6:2017	6	Ninguno	Implementar procesos seguros de instalación y utilizar procesos automatizados para verificar la efectividad de los ajustes y configuraciones en todos los ambientes.
Eventos no registrados, como credenciales de inicio de sesión fallidas.	Todas las Bases de datos.	A10:2017	4	ISO 12	Asegurarse que todos los errores de inicio de sesión, de control de acceso y de validación de entradas de datos se puedan registrar

Activos en Riesgos

- ✓ Base de datos Clientes
- ✓ Base de datos Proveedores
- ✓ Base de datos Cursos
- ✓ Base de datos Certificación

INFORME EJECUTIVO DE AUDITORIA

Viento en Popa es una importante empresa dentro del sector educativo Náutico el cual tiene un compromiso académico que buscan reflejar en acciones que garanticen la seguridad de sus operaciones en el corto plazo y cuyo objetivo es ser la mejor en su sector, por ello se realizó una serie de pruebas y análisis al portal web que es la herramienta principal de interacción entre sus clientes, personal administrativo y técnico.

Se enlistaron las principales pruebas y hallazgos que se obtuvieron en el proceso, así como los activos que están en riesgo, sus respectivos controles y las medidas posibles para contrarrestar el riesgo.

Actividades de auditoria:

- ✓ Realización de investigación previa de la empresa.
- ✓ Identificación de roles organizativos de Viento en Popa y su estructura organizacional.
- ✓ Identificación de controles
- ✓ Identificación de activos
- ✓ Presentación de Riesgos Inherentes al portal web.
- ✓ Realización de pruebas de seguridad al sitio web.
- ✓ Identificación de severidad y contramedidas de hallazgos

Hallazgos de intervención inmediata:

1. La aplicación utiliza datos que no son confiables en la construcción de varios comandos SQL lo cual generaría cualquier tipo de ataques comprometiendo al portal web.
2. El tiempo de vida de las sesiones de la aplicación no están configurados correctamente lo cual genera problemas de autenticación
3. Se utilizan hashes simples para almacenar las contraseñas de los usuarios lo cual generaría la exposición de datos confidenciales.
4. Problemas de registros y monitorización de eventos no registrados, como credenciales de inicio de sesión fallidas

BIBLIOGRAFÍA

27002, I. (mayo de 2017). *UNE-EN ISO/IEC 27002*. Obtenido de https://static.eoi.es/inline/une-en_iso-iec_27002_norma_mincotur.pdf

OWASP. (2017). Obtenido de <https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf>

Sentecal, S. (s.f.). *UNIR*. Obtenido de [https://micampus.unir.net/courses/22815/files/folder/Grupos%2039%20al%2042%20\(Sergio%20Sentecal\)/Actividad%3A%20El%20proceso%20y%20las%20fases%20de%20la%20auditoria%20de%20sistemas%20de%20informaci%C3%B3n?preview=4562987](https://micampus.unir.net/courses/22815/files/folder/Grupos%2039%20al%2042%20(Sergio%20Sentecal)/Actividad%3A%20El%20proceso%20y%20las%20fases%20de%20la%20auditoria%20de%20sistemas%20de%20informaci%C3%B3n?preview=4562987)