AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA JUGUETERÍAS HERMANOS BASKONIA.

TINA CALLEJA 27/03/2025

Tabla de contenido

1. Introducción.

La auditoría abarca la infraestructura tecnológica de la empresa, incluyendo la tienda online, los sistemas de comunicación, los equipos informáticos, y los sistemas de almacenamiento y seguridad tanto en la oficina principal como en el almacén.

Esta auditoría de seguridad tiene como objetivo implementar el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) para proteger los activos de la empresa y minimizar los riesgos de seguridad.

Jugueterías Hermanos Baskonia es una empresa de Vitoria con 10 empleados, dedicada al desarrollo y venta de juguetes.

La empresa cuenta con:

- Oficina principal
- Escaparate
- Almacén
- Mercado en línea para distribuir sus productos

2. Objetivos.

Los objetivos principales de la auditoría son:

1. Identificar los riesgos cibernéticos asociados con los activos de la empresa.
2. Establecer controles de seguridad apropiados y mejores prácticas de cumplimiento normativo.
3. Proporcionar recomendaciones para mitigar los riesgos y mejorar la seguridad general de la infraestructura.

Activos Gestionados por el Departamento de TI.

Los activos gestionados por el departamento de TI incluyen:

- Servidores y sistemas de almacenamiento de datos.
- Equipos de cómputo (PCs, laptops y dispositivos móviles).
- Plataforma de comercio electrónico (tienda online).
- Red local de oficina y sistemas de comunicación.

Inventario de Activos Tecnológicos.

Activo	*Cantidad*
Servidores físicos	*2*
Servidores virtuales	*5*
Sistemas de almacenamiento NAS	*3*
PCs de escritorio	*8*
Laptops	*6*
Tablets	*3*
Teléfonos móviles corporativos	*4*
Routers y switches de red	*5*
Firewalls	*2*
Cámaras de seguridad IP	*6*

Vulnerabilidades, riesgos y soluciones del departamento TI.

Los siguientes riesgos fueron identificados durante la auditoría:

- Pérdida de datos debido a vulnerabilidades en servidores y sistemas desactualizados.
- Posibles infecciones por malware debido a la falta de protección en equipos de escritorio.
- Accesos no autorizados a la red y cámaras de seguridad debido a configuraciones inseguras.

Control Evaluado	*Cumple (Sí/No)*	*Comentarios*	*Solución Propuesta*
Autenticación multifactor en sistemas críticos	*No*	*No implementado en todos los accesos.*	*Activar MFA en todas las cuentas administrativas.*
Actualización de software y parches	*No*	*Algunos servidores y PCs están desactualizados.*	*Aplicar actualizaciones de seguridad periódicas.*
Almacenamiento seguro de contraseñas	*No*	*Se guardan en texto plano.*	*Implementar hashing con bcrypt o Argon2.*
Configuración segura de routers	*No*	*Algunos routers tienen credenciales por defecto.*	*Actualizar configuraciones y credenciales.*
Segmentación de red	*Sí*	*Segmentación aplicada correctamente.*	*Mantener políticas de segmentación y acceso controlado.*

3. Análisis de la Plataforma de Comercio Electrónico.

Para evaluar la seguridad de la plataforma de comercio electrónico, se han utilizado las siguientes herramientas:

- *OWASP ZAP* : Se realizó un análisis automatizado de la aplicación web para detectar vulnerabilidades como inyección SQL y fallos en la autenticación.
- *BURP SUITE*: Se utilizó para realizar ataques de prueba contra formularios de inicio de sesión y detectar posibles fallos de seguridad.
- *NIKTO*: Se escaneó el servidor en busca de configuraciones inseguras y versiones obsoletas de software.

Vulnerabilidades, riesgos y soluciones del Comercio electrónico.

1. Falta de validación en formularios de ingreso de datos.
- Riesgo: Inyección de SQL o XSS.
- Solución: Implementar validaciones en el backend y sanitización de entradas.

2. Uso de HTTP en lugar de HTTPS en algunas páginas.
- Riesgo: Intercepción de datos sensibles.
- Solución: Forzar HTTPS en todo el sitio con redirecciones y certificados SSL.

3. Contraseñas almacenadas en texto plano.
- Riesgo: Compromiso de cuentas en caso de filtración.
- Solución: Implementar hashing seguro (bcrypt o Argon2).

Plataforma de Comercio Electrónico.

Control Evaluado	*Cumple (Sí/No)*	*Comentarios*	*Solución Propuesta*
Validación en formularios web	*No*	*Formularios vulnerables a inyección SQL/XSS.*	*Implementar validaciones y sanitización en backend.*
Uso de HTTPS en toda la web	*No*	*Algunas páginas aún usan HTTP.*	*Configurar redirecciones y aplicar certificados SSL.*
Protección contra ataques de inyección SQL/XSS	*No*	*Falta de validación en formularios.*	*Usar consultas parametrizadas y validación de entradas.*
Monitoreo y auditoría de accesos	*No*	*No hay un monitoreo activo de accesos.*	*Implementar auditoría y alertas de actividad sospechosa.*

4. Análisis de la Red Local de Oficina y Sistemas de Comunicación.

Para evaluar la seguridad de la red local, se utilizaron las siguientes herramientas:

Nmap: Para escanear puertos y detectar servicios expuestos. Wireshark: Para analizar el tráfico de red y detectar anomalías. OpenVAS: Para identificar vulnerabilidades en los dispositivos de red.

Vulnerabilidades, riesgos y soluciones de la red local.

No se encontraron vulnerabilidades críticas en la red local. Sin embargo, se recomienda:

- Mantener segmentada la red entre usuarios, servidores y dispositivos críticos.
- Implementar autenticación fuerte en dispositivos de red.
- Monitorear el tráfico regularmente en busca de posibles ataques.

Control Evaluado	*Cumple (Sí/No)*	*Comentarios*	*Solución Propuesta*
Firewall y control de accesos a la red	*Sí*	*Firewall implementado, pero sin auditorías regulares.*	*Realizar revisiones periódicas de las reglas de firewall.*
Monitoreo de tráfico en tiempo real	*No*	*No se analiza el tráfico de red regularmente.*	*Implementar herramientas como Wireshark o SIEM.*
Registro de actividades en la red	*No*	*No se registran accesos a la red.*	*Habilitar logs en routers y firewalls para auditoría.*

5. Seguridad del Almacén (NFC)

El almacén utiliza tarjetas NFC para el acceso, lo que introduce ciertos riesgos de seguridad.

Vulnerabilidades, riesgos y soluciones del almacén.

1. Clonación de tarjetas NFC.
- Riesgo: Un atacante podría duplicar una tarjeta y acceder al almacén.
- Solución: Usar autenticación de dos factores o tarjetas NFC con cifrado avanzado.

2. Falta de registro de accesos.
- Riesgo: No se puede auditar quién entra y sale.
- Solución: Implementar un sistema de registro con alertas en tiempo real.

Control Evaluado	*Cumple (Sí/No)*	*Comentarios*	*Solución Propuesta*
Registros de acceso al almacén NFC	*No*	*No se registra quién entra y sale.*	*Implementar un sistema de auditoría y alertas en tiempo real.*
Autenticación segura en sistemas de acceso	*No*	*Se usan tarjetas NFC sin autenticación adicional.*	*Implementar autenticación de dos factores.*
Protección contra clonación de tarjetas NFC	*No*	*Las tarjetas NFC pueden ser clonadas.*	*Usar tarjetas con cifrado avanzado y validación biométrica.*

6. Seguridad del Escaparate.

El escaparate no representa riesgos de ciberseguridad. Sin embargo, se recomienda verificar periódicamente su integridad física y asegurarse de que no haya dispositivos electrónicos sospechosos.

Vulnerabilidades, riesgos y soluciones del escaparate.

Control Evaluado	*Cumple (Sí/No)*	*Comentarios*	*Solución Propuesta*
Revisión de dispositivos electrónicos sospechosos	*No*	*No se realizan revisiones de seguridad.*	*Implementar inspecciones periódicas en el escaparate.*
Monitoreo de seguridad física del escaparate	*No*	*No hay sistema de monitoreo activo.*	*Instalar cámaras de seguridad con registro de actividad.*

7. Conclusión.

Esta auditoría ha identificado riesgos potenciales para los clientes, empleados y recursos de la empresa. Se han propuesto controles de seguridad y mejores prácticas para mitigar estos riesgos y cumplir con los estándares de ciberseguridad recomendados por el marco NIST.

8. Recomendaciones Finales

Para mejorar la ciberseguridad de Jugueterías Hermanos Baskonia, se recomienda implementar las siguientes acciones:

- Aplicar todas las soluciones propuestas en este informe.
- Realizar auditorías periódicas de seguridad en la plataforma de comercio electrónico.
- Establecer una política de seguridad para empleados y clientes.
- Monitorear la red y registrar actividad sospechosa.
- Mantener actualizados los sistemas y aplicar parches de seguridad.