**Auditoría Interna de Seguridad**

**Empresa: Electronics S.A.**

**Fecha: 08/06/2024**

**Auditor: Melina Noelia Mamani**

**Introducción**

Esta auditoría se realizó con el fin de evaluar los controles de seguridad y el cumplimiento de las mejores prácticas en Electronics S.A. La auditoría abarca diversos aspectos de la seguridad de la información y el cumplimiento de normativas relevantes.

**Evaluación de Controles de Seguridad**

A continuación, se presenta una lista de controles de seguridad evaluados. Marca con una "X" la columna correspondiente para indicar si el control está implementado.

| **Control** | **Implementado (Sí/No)** | **Explicación** |
| --- | --- | --- |
| Principio de Mínimo Privilegio | No | Todos los empleados tienen acceso a los datos de clientes; se debe limitar los privilegios para reducir el riesgo de brechas. |
| Planes de Recuperación ante Desastres | No | No existen planes de recuperación ante desastres. Estos deben implementarse para asegurar la continuidad del negocio. |
| Políticas de Contraseña | No | Las contraseñas de los empleados son mínimas, lo que podría permitir a un actor malintencionado acceder fácilmente a datos seguros. |
| Separación de Funciones | No | Debe implementarse para reducir la posibilidad de fraude/acceso a datos críticos. |
| Firewall | Sí | El firewall existente bloquea el tráfico basado en un conjunto de reglas de seguridad apropiadas. |
| Sistema de Detección de Intrusiones (IDS) | No | Se necesita un IDS para ayudar a identificar posibles intrusiones. |
| Copias de Seguridad | No | Se necesitan copias de seguridad de datos críticos para asegurar la continuidad del negocio en caso de una brecha. |
| Software Antivirus | Sí | El software antivirus está instalado y monitoreado regularmente por el departamento de TI. |
| Monitoreo y Mantenimiento de Sistemas Legados | No | Los sistemas legados se monitorean y mantienen, pero no hay un horario regular ni políticas claras para esta tarea, lo que podría poner en riesgo estos sistemas. |
| Cifrado | No | No se usa cifrado; su implementación proporcionaría mayor confidencialidad de la información sensible. |
| Sistema de Gestión de Contraseñas | No | No hay un sistema de gestión de contraseñas, su implementación mejoraría la productividad del departamento de TI y otros empleados. |
| Cerraduras (oficinas, tienda, almacén) | Sí | La ubicación física de la tienda tiene suficientes cerraduras. |
| CCTV | Sí | CCTV está instalado y funcionando en la ubicación física de la tienda. |
| Detección/Prevención de Incendios | Sí | La ubicación física tiene un sistema de detección y prevención de incendios funcional. |

**Evaluación de Cumplimiento**

Evalúa si la empresa cumple con las siguientes prácticas de cumplimiento.

**Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)**

| **Práctica** | **Cumplimiento (Sí/No)** | **Explicación** |
| --- | --- | --- |
| Solo usuarios autorizados tienen acceso a la información de las tarjetas de crédito de los clientes. | No | Todos los empleados tienen acceso a los datos internos de la empresa. |
| La información de las tarjetas de crédito se acepta, procesa, transmite y almacena de forma segura. | No | La información de las tarjetas no está cifrada y todos los empleados tienen acceso. |
| Implementar procedimientos de cifrado de datos. | No | La empresa no usa cifrado para asegurar la confidencialidad de la información financiera de los clientes. |
| Adoptar políticas de gestión de contraseñas seguras. | No | Las políticas de contraseñas son mínimas y no hay un sistema de gestión de contraseñas. |

**Reglamento General de Protección de Datos (GDPR)**

| **Práctica** | **Cumplimiento (Sí/No)** | **Explicación** |
| --- | --- | --- |
| Los datos de los clientes de la UE se mantienen privados/seguros. | No | La empresa no usa cifrado para asegurar la confidencialidad de la información financiera de los clientes. |
| Notificar a los clientes de la UE dentro de las 72 horas si sus datos son comprometidos. | Sí | Existe un plan para notificar a los clientes de la UE en caso de una brecha. |
| Asegurar que los datos están debidamente clasificados e inventariados. | No | Los activos actuales están inventariados, pero no clasificados. |
| Aplicar políticas de privacidad para documentar y mantener los datos. | Sí | Las políticas de privacidad fueron desarrolladas y aplicadas. |

**Controles de Sistemas y Organizaciones (SOC tipo 1 y tipo 2)**

| **Práctica** | **Cumplimiento (Sí/No)** | **Explicación** |
| --- | --- | --- |
| Políticas de acceso de usuario están establecidas. | No | No se implementaron controles de Mínimo Privilegio ni separación de funciones. |
| Los datos sensibles (PII/SPII) son confidenciales/privados. | No | No se usa cifrado para asegurar la confidencialidad de PII/SPII. |
| La integridad de los datos asegura que estos son consistentes, completos y validados. | Sí | La integridad de los datos está en su lugar. |
| Los datos están disponibles para los individuos autorizados. | No | Todos los empleados tienen acceso a los datos internos. |

**Recomendaciones**

Para mejorar la postura de seguridad de Electronics S.A. se deben implementar múltiples controles incluyendo: Principio de Mínimo Privilegio, planes de recuperación ante desastres, políticas de contraseñas, separación de funciones, un IDS, gestión continua de sistemas legados, cifrado y un sistema de gestión de contraseñas.

Para abordar las brechas de cumplimiento, se deben implementar controles como Principio de Mínimo Privilegio, separación de funciones y cifrado. Además, es necesario clasificar correctamente los activos para identificar controles adicionales que puedan mejorar la seguridad y proteger mejor la información sensible.