Check List Auditoría 2024-05-10 #1

Glow Clothing - San Lorenzo 3175 Eldorado

# Check List de Verificación de Controles

Seleccione “sí” o “no” para responder la pregunta: ¿Glow Clothing cuenta actualmente con este control?

| **Sí** | **No** | **Control** | ***Explicación*** |
| --- | --- | --- | --- |
|  |  | Privilegios mínimos | *Actualmente, todos los empleados tienen acceso a los datos de los clientes; Los privilegios deben limitarse para reducir el riesgo de una infracción.* |
|  |  | Planes de recuperación de desastres | *No existen planes de recuperación ante desastres. Estos deben implementarse para garantizar la continuidad del negocio.* |
|  |  | Políticas de contraseña | *Los requisitos de contraseña de los empleados son mínimos, lo que podría permitir que un actor de amenazas acceda más fácilmente a datos seguros/otros activos a través del equipo de trabajo de los empleados/la red interna.* |
|  |  | Separación de tareas | *Debe implementarse para reducir la posibilidad de fraude/acceso a datos críticos, ya que el director ejecutivo de la empresa actualmente dirige las operaciones diarias y administra la nómina.* |
|  |  | Cortafuegos | *El firewall existente bloquea el tráfico basándose en un conjunto de reglas de seguridad adecuadamente definidas.* |
|  |  |  |  |
|  |  | Sistema de detección de intrusos (IDS) | *El departamento de TI necesita un IDS para ayudar a identificar posibles intrusiones por parte de actores de amenazas.* |
|  |  | Copias de seguridad | *El departamento de TI necesita tener copias de seguridad de los datos críticos, en caso*  *de una infracción, para garantizar la continuidad del negocio.* |
|  |  | Software antivirus | *El departamento de TI instala y supervisa periódicamente el software antivirus.* |
|  |  | Monitoreo, mantenimiento e intervención manuales para sistemas heredados | *La lista de activos señala el uso de sistemas heredados. La evaluación de riesgos indica que estos sistemas son monitoreados y mantenidos, pero no existe un cronograma regular para esta tarea y los procedimientos/políticas relacionadas con la intervención no están claros, lo que podría poner a estos sistemas en riesgo de sufrir una violación.* |
|  |  | Cifrado | *Actualmente no se utiliza cifrado; implementarlo proporcionaría una mayor confidencialidad de la información sensible.* |
|  |  | Sistema de gestión de contraseñas | *Actualmente no existe ningún sistema de gestión de contraseñas; La implementación de este control mejoraría la productividad del departamento de TI y de otros empleados en caso de problemas con las contraseñas.* |
|  |  | Cerraduras (oficinas, escaparate, almacén) | *La ubicación física de la tienda, que incluye las oficinas principales de la empresa, el frente de la tienda y el almacén de productos, cuenta con cerraduras suficientes.* |
|  |  | Vigilancia por circuito cerrado de televisión (CCTV) | *CCTV está instalado/funcionando en la ubicación física de la tienda.* |
|  |  | Detección/prevención de incendios (alarma de incendios, sistema de rociadores, etc.) | *La ubicación física de Glow Clothing cuenta con un sistema de detección y prevención de incendios en funcionamiento.* |

# 

# Check List de Verificación de Cumplimiento

Seleccione “sí” o “no” para responder la pregunta: Glow Clothing cumple actualmente con estas mejores prácticas de cumplimiento?

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

| **Sí** | **No** | **Mejores prácticas** | ***Explicación*** |
| --- | --- | --- | --- |
|  |  | Sólo los usuarios autorizados tienen acceso a la información de la tarjeta de crédito de los clientes. | *Actualmente, todos los empleados tienen acceso a los datos internos de la empresa.* |
|  |  | La información de la tarjeta de crédito se acepta, procesa, transmite y almacena internamente, en un entorno seguro. | *La información de la tarjeta de crédito no está cifrada y actualmente todos los empleados tienen acceso a los datos internos, incluida la información de la tarjeta de crédito de los clientes.* |
|  |  | Implemente procedimientos de cifrado de datos para proteger mejor los datos y los puntos de contacto de las transacciones con tarjetas de crédito. | *Actualmente, la empresa no utiliza cifrado para garantizar mejor la confidencialidad de la información financiera de los clientes.* |
|  |  | Adopte políticas seguras de gestión de contraseñas. | *Las políticas de contraseñas son nominales y actualmente no existe ningún sistema de administración de contraseñas.* |

Reglamento General de Protección de Datos (GDPR)

| **Sí** | **No** | **Mejores prácticas** | ***Explicación*** |
| --- | --- | --- | --- |
|  |  | UE. Los datos de los clientes se mantienen privados/seguros. | *Actualmente, la empresa no utiliza cifrado para garantizar mejor la confidencialidad de la información financiera de los clientes.* |
|  |  | Existe un plan para notificar a la UE. a los clientes en un plazo de 72 horas si sus datos se ven comprometidos/hay una infracción. | *Existe un plan para notificar a la UE. clientes dentro de las 72 horas posteriores a una violación de datos.* |
|  |  | Asegúrese de que los datos estén clasificados e inventariados adecuadamente. | *Los activos corrientes han sido inventariados/cotizados, pero no clasificados.* |
|  |  | Hacer cumplir políticas, procedimientos y procesos de privacidad para documentar y mantener adecuadamente los datos. | *Se han desarrollado y aplicado políticas, procedimientos y procesos de privacidad entre los miembros del equipo de TI y otros empleados, según sea necesario.* |

Controles de sistemas y organizaciones (SOC tipo 1, SOC tipo 2)

| **Sí** | **No** | **Mejores prácticas** | ***Explicación*** |
| --- | --- | --- | --- |
|  |  | Se establecen políticas de acceso de usuarios. | *Actualmente no existen controles de privilegios mínimos ni separación de funciones; todos los empleados tienen acceso a los datos almacenados internamente.* |
|  |  | Los datos confidenciales (PII/SPII) son confidenciales/privados. | *Actualmente no se utiliza el cifrado para garantizar mejor la confidencialidad de la PII/SPII.* |
|  |  | La integridad de los datos garantiza que los datos sean coherentes, completos, precisos y hayan sido validados. | *La integridad de los datos está vigente.* |
|  |  | Los datos están disponibles para las personas autorizadas a acceder a ellos. | *Si bien los datos están disponibles para todos los empleados, la autorización debe limitarse únicamente a las personas que necesitan acceder a ellos para realizar su trabajo.* |

# Recomendaciones

En esta sección, se establecen recomendaciones relacionadas con controles y/o necesidades de cumplimiento que su gerente de TI podría comunicar a las partes interesadas para reducir los riesgos para los activos y mejorar la postura de seguridad de Glow Clothing:

*Es necesario implementar múltiples controles para mejorar la postura de seguridad de Glow Clothing y garantizar mejor la integridad de la información confidencial, incluidos:*

* Política de privilegios mínimos
* Planes de recuperación ante desastres
* Políticas de contraseñas
* Separación de funciones
* Implementación de un IDS
* Administración continua de sistemas heredados
* Cifrado
* Implementación de un sistema de gestión de contraseñas

*Para abordar las brechas en el cumplimiento, Glow Clothing necesita implementar controles como Mínimos Privilegios, separación de funciones y cifrado. La empresa también necesita clasificar adecuadamente los activos para identificar controles adicionales que puedan necesitar implementarse para mejorar su postura de seguridad y proteger mejor la información confidencial.*