**Programación Segura.**

**Incorporación de 27001 en Less Row**

**1. Introducción**

Este informe detalla la implementación estándar ISO 27001 en el sistema de gestión de Less Row, una plataforma para gestionar accesos, tickets y reservas en un parque de atracciones. La ISO 27001 establece un marco de trabajo para proteger la información sensible, garantizar la seguridad de los datos y mitigar riesgos asociados a la gestión digital de la información.

**2. Objetivos de la Implementación**

1. Asegurar la confidencialidad, integridad y disponibilidad de la información:
   * Proteger los datos personales y financieros de los visitantes.
   * Garantizar que los servicios de la plataforma estén siempre disponibles.
2. Cumplir con regulaciones legales y normativas locales.

* Prohibir el uso de datos personales sin el consentimiento de los titulares.

1. Incrementar la confianza de los visitantes:
   * Garantizando que su información está bien protegida.
2. Prevenir y mitigar riesgos de seguridad:
   * Ciberataques, accesos no autorizados o errores humanos.

**3. Fases de Implementación**

**3.1. Fase de Evaluación Inicial**

* Análisis de riesgos:
  + Identificar las amenazas que pueden afectar los datos manejados, como:
    - Robo de información de visitantes.
    - Acceso no autorizado al sistema.
    - Pérdida de datos en caso de fallos técnicos.
  + Clasificar los riesgos en función de su impacto y probabilidad.
* Identificación de activos:
  + Datos sensibles: información personal de visitantes, códigos QR y datos de pago.
  + Recursos tecnológicos: bases de datos, servidores y dispositivos de escaneo.

**3.2. Fase de Planificación**

* Definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI):
  + Abarcar las áreas críticas: generación de tickets, verificación de accesos y gestión de pagos.
* Establecer políticas de seguridad:
  + Definir cómo se manejará la información.
  + Asegurar que solo personal autorizado tenga acceso.

**3.3. Fase de Implementación**

* Controles técnicos:
  + Cifrado de datos personales y financieros.
  + Uso de autenticación multifactor para el acceso al sistema.
  + Monitoreo continuo para detectar actividades sospechosas.
* Capacitación del personal:
  + Entrenar a los funcionarios en buenas prácticas de seguridad, como:
    - Uso adecuado de los dispositivos de escaneo.
    - Identificación de intentos de acceso no autorizado.
  + Realizar simulaciones de posibles incidentes de seguridad.



* Gestión de acceso:
  + Restringir el acceso a datos sensibles solo a quienes lo necesiten.
  + Implementar controles de acceso físico para proteger los dispositivos utilizados.

**3.4. Fase de Validación y Monitoreo**

* Realizar auditorías internas periódicas para comprobar que se cumplen las políticas de seguridad.
* Monitorear el desempeño del sistema y registrar cualquier incidente de seguridad.
* Mejorar continuamente el SGSI según los resultados obtenidos.

**4. Beneficios Obtenidos**

1. Mayor seguridad en los procesos:
   * Los datos de los visitantes, como información personal y de pagos, están protegidos contra accesos no autorizados.
2. Cumplimiento legal y normativo:
   * La implementación de la ISO 27001 asegura que se cumplan normativas de protección de datos, como la Ley de Protección de Datos Personales en Chile.
3. Confianza de los clientes:
   * Los visitantes confían en que sus datos están seguros al utilizar la plataforma Less Row.
4. Reducción de riesgos:
   * Se disminuyó el impacto potencial de ciberataques y errores humanos.
5. Procesos optimizados:
   * Se logró una mejor organización en la gestión de la información y se redujeron errores operativos.

**5. Ejemplo Práctico en Less Row**

* Verificación de códigos QR:
  + Los códigos QR de los visitantes ahora están cifrados y se validan en tiempo real mediante servidores seguros.
  + Los funcionarios usan dispositivos con controles de acceso para evitar que personas no autorizadas puedan escanear códigos.
* Gestión de pagos:
  + Las transacciones están protegidas mediante cifrado y los datos financieros no se almacenan en el sistema, sino que son manejados por plataformas certificadas como.

Imagen que contiene Aplicación

Descripción generada automáticamente