

# Informe KPI

Alexys Gomez Elizalde

## Introducción

La tienda online de Juan Pérez, que se dedica a la venta de productos electrónicos, enfrenta riesgos significativos que tienen que ver con ataques cibernéticos y la pérdida de datos por errores humanos. Estos riesgos pueden comprometer la seguridad de la información de los clientes y la continuidad de las operaciones. A continuación, se detallan las estrategias propuestas para monitorizar y mitigar estos riesgos utilizando indicadores clave de rendimiento (KPIs).

## Objetivos

- **Mitigar el impacto de ataques cibernéticos** en la plataforma de ventas en línea.
- **Reducir la probabilidad y el impacto de la pérdida de datos** causada por errores humanos.
- **Asegurar la continuidad y seguridad de las operaciones** de la tienda.

## KPIs Seleccionados

- Número de intentos de acceso no autorizado detectados.
- Tiempo de respuesta a incidentes cibernéticos.
- Cantidad de incidentes de pérdida de datos reportados.
- Tasa de recuperación de datos exitosos después de un incidente.

## Estrategias Propuestas

### 1. Implementación de Firewalls Avanzados y Sistemas de Detección de Intrusiones (IDS)

**Acción:** Instalar firewalls avanzados y sistemas de detección de intrusiones para monitorear y bloquear intentos de acceso no autorizados. El sistema IDS alertará al equipo de TI en tiempo real sobre cualquier actividad sospechosa.

#### **Impacto en KPIs:**

- **Reducción del Número de Intentos de Acceso No Autorizado:** Los firewalls y el IDS proporcionarán una línea de defensa que minimiza los intentos de ataque exitosos.
- **Mejora en el Tiempo de Respuesta a Incidentes:** Con alertas en tiempo real, el equipo técnico puede responder de manera inmediata a las amenazas.

### 2. Capacitación Continua en Seguridad y Protocolos de Manejo de Datos

**Acción:** Establecer un programa de capacitación continua para el personal, centrado en la seguridad de la información y la correcta manipulación de datos sensibles. Este programa incluirá simulaciones de ataques y ejercicios de recuperación de datos.

#### **Impacto en KPIs:**

- **Reducción de la Cantidad de Incidentes de Pérdida de Datos:** La capacitación mejora la conciencia y habilidades del personal, disminuyendo la ocurrencia de errores humanos.

- **Incremento en la Tasa de Recuperación de Datos Exitosos:** El personal entrenado puede seguir protocolos de recuperación de datos de manera efectiva en caso de incidentes.

### 3. Implementación de Respaldo Automatizado de Datos

**Acción:** Configurar un sistema de respaldo automatizado de datos críticos, con copias almacenadas tanto en localizaciones físicas distintas como en la nube. El sistema realizará copias de seguridad periódicas y pruebas de restauración regulares.

**Impacto en KPIs:**

- **Minimización de la Pérdida de Datos:** Un sistema de respaldo automatizado asegura que los datos críticos se recuperen rápidamente, incluso después de un error humano o ciberataque.
- **Aumento de la Tasa de Recuperación de Datos Exitosos:** Al tener un respaldo actualizado, la restauración de datos en caso de pérdida es más efectiva.

### 4. Auditoría y Revisión Regular de Seguridad

**Acción:** Realizar auditorías de seguridad periódicas para evaluar la efectividad de las medidas implementadas y actualizar los sistemas y protocolos según las nuevas amenazas y vulnerabilidades.

**Impacto en KPIs:**

- **Reducción Continua de Amenazas:** Las auditorías permiten identificar y corregir vulnerabilidades antes de que sean explotadas.
- **Mejora en el Tiempo de Respuesta a Incidentes:** La revisión continua optimiza los protocolos de respuesta, asegurando que el equipo esté preparado para enfrentar cualquier incidente.

## Implementación

**Cronograma:** La instalación de firewalls y sistemas IDS comenzará inmediatamente, con una duración estimada de un mes. La capacitación del personal y la implementación de respaldos automatizados se programarán para los próximos dos meses.

**Presupuesto:** Se asignará un presupuesto para la compra de software y hardware de seguridad, así como para la contratación de expertos en ciberseguridad para la capacitación del personal.

**Responsables:** El equipo de TI será responsable de la implementación técnica y el mantenimiento de las medidas de seguridad, mientras que el departamento de operaciones supervisará el cumplimiento del cronograma y el uso del presupuesto.

## Conclusión

La implementación de estas medidas permitirá a la tienda de Juan Pérez no solo mitigar los riesgos relacionados con ciberataques y la pérdida de datos, sino también fortalecer la resiliencia de su plataforma en línea, asegurando la continuidad de sus operaciones y la protección de la información de sus clientes.