ISO 27001
Actividad

INTEGRANTES:

- Lisandra Durán Romero.
- Ian Anthony Pérez González.
- Evelyn Damarys Pulido Méndez.
- Omar Imanol Rodríguez Rodríguez.

FACULTAD DE TELEMÁTICA
Ingeniería en Software
5°I

14/11/2025

Dashboard de Riesgos del SGSI Steren

El *dashboard* servirá como una herramienta de gestión para la Alta Dirección y los dueños de riesgos, visualizando la **exposición actual de Steren a amenazas de seguridad** y el progreso en la implementación de las acciones de tratamiento.

1. Indicadores de Riesgo (Risk Exposure)

Esta sección muestra el nivel de riesgo actual de la organización, utilizando la información de la Matriz de Riesgos de la Cláusula 6.1.2.

- **Riesgo Inherente Total:**
    - **Visualización:** Un único indicador que muestra la suma o el promedio ponderado de todos los riesgos antes de aplicar cualquier control (el "peor escenario").
    - **Propósito:** Proporcionar una visión de la exposición bruta de Steren.
- **Riesgo Residual Prioritario:**
    - **Visualización:** Una lista que enumera los **3 a 5 riesgos principales de Steren** que, *después* de aplicar los controles, aún presentan un nivel de riesgo "Alto" o "Medio" (ej. R02: Fuga de Datos de Clientes).
    - **Propósito:** Enfocar la atención de la dirección en las áreas que requieren más recursos o aprobación de riesgo.
- **Distribución de Riesgos por Tipo de Activo:**
    - **Visualización:** Una lista que muestra cómo se distribuyen los riesgos entre los principales activos de Steren.
    - **Componentes:**
        - Riesgos en **Sistemas de Punto de Venta (POS)**.
        - Riesgos en **Plataforma E-commerce y Nube**.
        - Riesgos en **Inventario Físico y CEDIS**.

2. Estado de Tratamiento de Riesgos (Control Implementation Progress)

Esta sección refleja el Plan de Tratamiento de Riesgos (PTR - Cláusula 6.1.3), mostrando el progreso en la implementación de las Políticas A y B y otros controles seleccionados.

- **Progreso de Implementación del PTR:**
    - **Visualización:** Una barra de progreso o un indicador porcentual del total de acciones definidas en el PTR.
    - **Propósito:** Medir la eficiencia del equipo de TI en la aplicación de las acciones de mitigación planificadas.
- **Estado de las Políticas Críticas:**
    - **Visualización:** Un semáforo o indicador para cada política principal.
    - **Componentes:**

        - **Política A (Seguridad Física):** Porcentaje de sucursales con control de acceso biométrico implementado (Ref. Control 7.2) y CCTV en funcionamiento (Ref. Control 7.4).
        - **Política B (Uso Seguro de POS):** Porcentaje de terminales con filtrado web activo (Ref. Control 8.23) y uso de credenciales únicas forzado (Ref. Control 5.15).
- **Eficacia de Controles (KPIs de Riesgo):**
    - **Visualización:** Indicadores clave que miden si los controles están funcionando.
    - **Ejemplo:** Número de intentos de acceso no autorizado detectados por el CCTV (Ref. Control 7.4) o el índice de clics en correos de *phishing* (Ref. Control 6.3).

3. Aprobación y Responsabilidad (Accountability)

Esta sección se centra en los requerimientos de liderazgo y responsabilidad (Cláusula 5.3 y 6.1.3 f)).

- **Riesgos Pendientes de Aprobación:**
    - **Visualización:** Un contador que muestra cuántos riesgos residuales (riesgos que Steren ha decidido aceptar) están pendientes de ser aprobados formalmente por los dueños de riesgos o la Alta Dirección.
- **Dueños de Riesgos con Acciones Atrasadas:**
    - **Visualización:** Una lista que identifica a los roles o gerentes (dueños de riesgos) que tienen acciones de tratamiento de riesgo (PTR) que han excedido su fecha límite planificada.

En resumen, el *dashboard* transforma la documentación densa de la Matriz de Riesgos en un **tablero de salud de seguridad**, permitiendo a la dirección de Steren tomar decisiones rápidas sobre dónde asignar tiempo y presupuesto.

Política A: Política de Seguridad Física y Protección de Inventario

Propósito: Proteger los activos tecnológicos de alto valor en almacenes y el acceso a las áreas restringidas de las sucursales.

Declaración de la Política:

1. **Zonas de Acceso Restringido (Ref. Control 7.2):** El acceso a las bodegas de inventario en sucursales y CEDIS (Centros de Distribución) está estrictamente limitado al personal de almacén y gerencia. Se deben utilizar controles físicos de entrada (biométricos, tarjetas o llaves controladas) validados por la Dirección .

2. **Videovigilancia Continua (Ref. Control 7.4):** Todas las instalaciones (tiendas y perímetro de almacenes) deben ser monitorizadas continuamente mediante sistemas de CCTV para detectar accesos no autorizados y prevenir la pérdida de activos .
3. **Protección de Equipos (Ref. Control 7.8):** Los equipos de demostración y los servidores de las tiendas deben situarse de forma protegida para evitar robos o manipulaciones no autorizadas por parte de clientes o terceros .

Política B: Política de Uso Seguro de Puntos de Venta (POS) y E-commerce

Propósito: Asegurar que las transacciones de venta sean seguras y que los datos de los clientes (tarjetas, direcciones) no sean comprometidos.

Declaración de la Política:

1. **Uso Aceptable de Equipos de Venta (Ref. Control 5.10):** Las computadoras y terminales de punto de venta (POS) son para uso exclusivo de actividades comerciales de Steren. Está prohibido su uso para navegación personal, redes sociales o descarga de software no autorizado .
2. **Filtrado de Navegación (Ref. Control 8.23):** El departamento de TI implementará restricciones técnicas (filtrado web) en la red de las sucursales para bloquear el acceso a sitios web maliciosos o no relacionados con el negocio .
3. **Control de Accesos a Sistemas (Ref. Control 5.15):** Cada vendedor y cajero debe tener un usuario y contraseña únicos para acceder al sistema de ventas. Queda prohibido compartir credenciales genéricas como "Caja1" .
4. **Protección de Datos en la Nube (Ref. Control 5.23):** La gestión de la tienda en línea y los datos de clientes alojados en la nube deben seguir procesos de adquisición y gestión que cumplan con los requisitos de seguridad de la información definidos por la organización (encriptación, backups) .