





**IMPLEMENTACION DE POLITICAS DE SEGURIDAD**

**Datos de la Empresa:** CBA

**Descripción:** Fundación americana de idiomas

**Tamaño de la Empresa:** 20 empleados

**Principales Activos de Información:** Cámaras

**Principales Riesgos de Seguridad:** Daño físico

**Paso 1: Inventario de Activos de Información**

**Descripción:** El primer paso en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es realizar un inventario completo de todos los activos de información de la empresa. Esto implica identificar y enumerar todos los sistemas, datos y recursos que son críticos para las operaciones de la empresa y que requieren protección contra amenazas de seguridad.

1. Identificación de Activos de Información

Cámaras

1. Clasificación de Activos

Alta

1. Documentación de inventario

| **Tipo de activo** | **Descripción** | **Ubicación** | **Propietario** | **Sensibilidad** |
| --- | --- | --- | --- | --- |
| Cámara | Cámara de seguridad | Corredores | Departamento de IT | Alta |

**Paso 2: Evaluación de Riesgo**

**Descripción:** La evaluación de riesgos es un proceso fundamental en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Consiste en identificar y analizar las amenazas y vulnerabilidades que pueden afectar a los activos de información de la empresa, así como evaluar el impacto y la probabilidad de ocurrencia de dichos riesgos.

1. **Identificación de amenazas**

Vandalismo

1. **Análisis de Vulnerabilidades**

Mal ubicación

1. **Evaluación de impacto**

Dificultad de investigaciones

1. **Evaluación de probabilidad**

Vandalismo: Alta debido al mal posicionamiento de la cámara, ubicación baja.

1. **Priorización de riesgos**

Crítico

**Paso 3: Diseño de controles de Seguridad**

**Descripción:** Una vez que se han identificado los riesgos de seguridad en el paso anterior, el siguiente paso es diseñar e implementar controles de seguridad adecuados para mitigar estos riesgos. Los controles de seguridad son medidas técnicas, organizativas o administrativas que se implementan para proteger los activos de información de una empresa contra amenazas de seguridad.

1. **Selección de controles**

Revisión de las normas

1. **Diseño de control técnico**

Cámaras en ubicación inalcanzable

1. **Desarrollo de controles organizativos**

Política de Acceso: Establece los requisitos y procedimientos para el acceso a los sistemas y datos de la empresa, incluyendo la autenticación y autorización.

1. **Implementación de controles**

Implementación de sensores: Configurar sensores de movimiento para monitorear posibles ataques físicos.

1. **Monitoreo y Mantenimiento de Controles:**

Monitoreo continuo: Supervisar la integridad de dichas cámaras

**Paso 4: Desarrollo de Políticas y Procedimientos de Seguridad de la Información**

**Descripción:** El desarrollo de políticas y procedimientos de seguridad de la información es esencial para establecer las normas y prácticas que guiarán el manejo seguro de los activos de información de la empresa. Estas políticas y procedimientos proporcionan un marco de referencia para la toma de decisiones y la gestión de la seguridad de la información en la organización.

1. **Análisis de Requisitos y Regulaciones**

Las cámaras deben ser resistentes al vandalismo y a condiciones climáticas extremas (IP66), tener el herraje apropiado para su montaje, y soportar temperaturas entre -35°C a 60°C. La conexión de entrada debe ser compatible con RJ45 10BASE-T/100BASE-TX, y la alimentación con PoE.

1. **Definición de objetivos de seguridad**

**Fortalecer la Seguridad Física:** Integrar la instalación de cámaras de seguridad con medidas de seguridad física, como sistemas de control, elementos del entorno y control de acceso, para crear un ambiente seguro y disuasorio para posibles actos vandálicos.

**Desarrollo de Políticas de Seguridad**

**Política de Gestión de Buenas Prácticas para la Instalación de Cámaras de seguridad.**

**Objetivo:** Esta política establece los estándares y normativas para la instalación de cámaras de seguridad en el CBA Centro Americano Boliviano de Idiomas, con el fin de asegurar la integridad y seguridad audiovisual de la institución, minimizando el riesgo de vandalismo y garantizando la eficacia del sistema de vigilancia

**Alcance:** Esta política aplica a las instalaciones del CBA Centro Americano Boliviano de Idiomas, con el objetivo de proteger los activos culturales, educativos y personales de la institución.

**Directrices:**

**Planificación Estratégica:**Antes de iniciar la instalación, se debe realizar una planificación detallada que identifique los puntos críticos para la colocación de cámaras que maximicen la cobertura y la eficacia contra el vandalismo, considerando las áreas de mayor tráfico y las áreas sensibles como bibliotecas y salas de estudio.

**Formación y Capacitación:**Los encargados de la instalación de cámaras de seguridad deben estar capacitados en las buenas prácticas de instalación y ser responsables de garantizar la resistencia al vandalismo en todas las instalaciones.

1. **Elaboración de Procedimientos de seguridad**

**Identificación del Incidente**

**Detección:** Las cámaras de seguridad detectan actividad inusual o daño.

**Registro:** Se registra la fecha, hora, ubicación y detalles del incidente.

**Evaluación del Incidente**

**Análisis de la grabación:** Se revisa la grabación de la cámara para identificar el acto de vandalismo.

**Determinación de la Severidad:** Se evalúa el daño causado y su impacto en la institución.

**Notificación**

**Informar a la Administración:** Se informa a la administración de la institución sobre el incidente.

**Comunicación con las Autoridades:** En casos graves, se informa a las autoridades locales.

**5. Revisión y aprobación**

**Dirección Ejecutiva:** Revisión y aprobación final de las políticas y

procedimientos.

**Departamento de IT:** Revisión de procedimientos técnicos para garantizar su

viabilidad y eficacia.

**Paso 5: Elaboración del Plan de Implementación del SGSI**

**Descripción:** El plan de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) es un documento detallado que describe cómo se llevará a cabo la implementación de las políticas, procedimientos y controles de seguridad de la información en la empresa. Este plan proporciona una hoja de ruta clara para garantizar que el SGSI se implemente de manera efectiva y eficiente.

1. **Definición de Roles y Responsabilidades**
2. **Establecimiento de Metas y Objetivos**
3. **Desarrollo de un Cronograma**
4. **Asignación de Recursos**
5. **Desarrollo de Mecanismos de Evaluación**