**IDENTIFICACIÓN DE RIESGOS**

**Mariana Cifuentes Londoño**

**Código: 1.005.091.500**

**Santiago Maya Cortés**

**Código: 1.092.850.328**

**José Alejandro Zambrano Jiménez**

**Código: 1.010.090.406**

****

**Profesora: Andrea Viveros Quisoboni**

**Universidad del Quindío  
Facultad de Ingeniería**

**Ingeniería de Sistemas y Computación**

**Seguridad en Infraestructura de TI**

**Grupo: 01-D**

**Armenia, Quindío, 2023**

**Vulnerabilidades**

* Puesto de trabajo desatendido.
* Objetos personales expuestos.
* Seguridad de los Sistemas de Información comprometida.
* Consumo de alimentos en área sensible.
* Exposición de credenciales de usuario

**Amenazas**

* Pérdida de la confidencialidad debido a la facilidad de accesos no autorizados a la información disponible en el escritorio.
* Pérdida de la integridad por el acceso no autorizado a los sistemas de información.
* Pérdida de disponibilidad por sistemas de información expuestos.
* Ataque cibernético por ingreso de virus informáticos como malware al sistema empresarial.
* Infiltración a la red de la empresa

**Riesgos**

* Robo de información de la empresa.
* Infiltración en los Sistemas de Información.
* Daño en los activos físicos.
* Robo o daño de elementos personales.
* Acceso no autorizado al Data Center u otras dependencias de la organización

**Probabilidad**

* Robo de información - 90%
* Infiltración en los Sistemas de Información - 90%
* Daño en los activos físicos - 70%
* Robo o daño de elementos personales - 90%
* Acceso no autorizado al Data Center u otras dependencias de la organización - 70%

**Impacto**

* Divulgación no autorizada de datos sensibles
* Perdida de dinero por objetos personales
* Pérdida de recursos financieros debido a ataques
* Daño a la reputación de la empresa por escándalos de falta de seguridad.
* Daño a los activos por consumo de alimentos
* Pérdida de clientes y disminución de confianza en la empresa.

**Controles**

* Bloqueo de equipos después de cierto tiempo de inactividad
* Almacenamiento de activos físicos en lugares autorizados y seguros
* Establecer espacios para guardar elementos personales
* Implementar zonas de consumo de alimentos fuera de las oficinas
* Monitorear acceso físico a las oficinas