# Angel Luis Garcia-Junco Lora

# Actividad Práctica 1: Evaluación y aplicación de medidas de seguridad según la norma ISO/IEC 27002

## Enunciado:

Eres parte del equipo de seguridad informática de una empresa que está implementando un sistema de gestión de la seguridad de la información. La dirección te ha encargado identificar riesgos potenciales y proponer medidas basadas en la norma ISO/IEC 27002, siguiendo las secciones principales del estándar.

## Tareas:

1. Identifica tres posibles riesgos relacionados con:

* - Seguridad física del entorno
* - Gestión de activos
* - Seguridad ligada a los recursos humanos

2. Relaciona cada riesgo con una medida de control recomendada por la norma ISO/IEC 27002.

3. Justifica la selección de cada medida indicando su utilidad y cómo contribuye a minimizar el riesgo identificado.

En detalle:

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo identificado** | **Tipo** | **Medida de control propuesta** | **Justificación** |
| No hay control de acceso a los ascensores | Seguridad física del entorno | Incorporar un control biométrico de acceso al ascensor | Que no pueda acceder personal no autorizado a las plantas con activos sensibles de la empresa |
| No se eliminan adecuadamente los activos sensibles cuando han terminado su ciclo de vida | Gestion de activos | Llevar un control exhaustivo del ciclo de vida de cada activo, mediante una alerta de sistema para el responsible de cada departamento propietario del activo | Cumplir con la ley de proteccion de datos ademas de la iso 27002 completando el ciclo de vida del activo |
| Los empleados no estan capacitados para su desempeño, en concreto, hay quejas del responsible de tratamiento de datos | Seguridad ligada a los recursos humanos | Capacitar a los empleados con formaciones y pruebas practicas en sandbox periodicas, y si no la superan redistribuir al personal white collar, al menos que haya 3 en el puesto de responsible de datos, el Aprendiz , el Junior y el Senior, que vayan ascendiendo, o siendo sustituidos, dependiendo del resultado de sus capacitaciones. | Asegurar la correcta cualificación, capacidad y evolucion del personal en su desempeño en el puesto de trabajo |

En resumen con el siguiente formato:

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo identificado** | **Sección de la norma ISO/IEC 27002** | **Medida de control propuesta en norma** | **Justificación** |
| Ausencia de control de acceso | Seguridad física del entorno | Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado. | Minimizar el riesgo de acceso de personal no autorizado |
| Existencia de activos sensibles al final de su ciclo de vida | Gestion de activos | Asegurar ciclo de vida de los activos | Cumplir con la LOPDGDD |
| Capacitacion insuficiente de empleados | Seguridad ligada a los recursos humanos | Concienciación, educación y capacitación en seguridad de la información | Asegurar una capacitacion adecuada, con un mínimo de conocimientos |