**Ejercicio en Clase:**

**Análisis del Alcance para una Certificación ISO/IEC 27002:2022**

**Objetivos:**

* Comprender y definir el alcance y entendimiento de la organización en relación con la implementación de controles de seguridad de la información requeridos por ISO/IEC 27002:2022.
* Desarrollar competencias específicas para la implementación de un SGSI bajo estándares internacionales, reforzando habilidades de análisis, trabajo en equipo y aplicación práctica.

**Duración:**

60 minutos (30 minutos para trabajo en grupo, 20 minutos para presentación y 10 minutos para discusión).

**Instrucciones**

**Contexto:**

Supongamos que tu organización está buscando certificarse en ISO/IEC 27001:2022 (apoyada por los controles de la ISO/IEC 27002:2022). Para ello, el primer paso es definir claramente el alcance del Sistema de Gestión de Seguridad de la Información (SGSI). Esto incluye identificar los activos clave, las partes interesadas y los requisitos legales y normativos.

**Actividad:**

1. **Formación de equipos:** Divide a los estudiantes en grupos de 4-5 personas. Cada equipo asumirá el rol de consultores externos contratados por una empresa ficticia.
2. **Caso de estudio:** La empresa ficticia es "TechGuard S.A.S.", una organización de tecnología con las siguientes características:

* Ofrece servicios en la nube para pequeñas y medianas empresas.
* Maneja datos sensibles de clientes en servidores distribuidos globalmente.
* Cuenta con 3 oficinas físicas en Bogotá, Medellín y Cali.
* Emplea a 150 personas, de las cuales el 40% trabaja de forma remota.
* Tiene que cumplir con regulaciones como la Ley 1581 de 2012 (protección de datos en Colombia).

1. **Tareas a realizar (30 minutos):** Cada equipo debe:

* **Definir el alcance del SGSI** considerando los activos, las ubicaciones, los procesos y las partes interesadas relevantes.
* Identificar **principales riesgos** asociados a la seguridad de la información en la organización.
* Relacionar los **dominios clave de ISO/IEC 27002:2022** que consideran prioritarios para esta empresa.
* Proponer un primer borrador del alcance del SGSI (máximo 5-7 líneas).

1. **Presentación (20 minutos):** Cada equipo presentará su alcance y análisis al resto de la clase.
2. **Discusión (10 minutos):** Entre todos, se compararán los enfoques y se seleccionará el alcance mejor definido según los principios de ISO/IEC 27002:2022.

**Material de apoyo:**

* Fragmento del estándar ISO/IEC 27002:2022 relacionado con los dominios clave y controles.
* Guía resumen de los principios de la Ley 1581 de 2012.

**Criterios de evaluación:**

1. **Relevancia del alcance:**
2. El alcance incluye activos, ubicaciones y procesos clave.
3. **Identificación de riesgos:**
4. Se identificaron riesgos críticos y realistas para la organización.
5. **Relación con ISO/IEC 27002:2022:**
6. Se priorizaron dominios y controles relevantes al caso.
7. **Claridad y precisión:**
8. El alcance está redactado de forma clara y concisa.