UNIVERSIDAD DE LAS FUERZAS ARMADAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

INGENIERÍA ENT TECNOLOGÍAS DE LA INFORMACIÓN

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

PARCIAL 2

TEMA: Alcance del SGSI

FECHA: 13 de enero del 2025

INTEGRANTES:

- Castro Bryan
- Torres Marloln

Contenido

1. Descripción de la Organización

La infraestructura tecnológica de XYZ opera principalmente en Microsoft Azure, una plataforma de nube pública que cumple con los estándares de seguridad internacionales y está certificada bajo la norma ISO 27001. Esta configuración plantea retos significativos para la seguridad de la información, lo que llevó a la organización a adoptar la norma ISO 27001 como marco para su Sistema de Gestión de Seguridad de la Información (SGSI).

Pablo, el CTO de la empresa, lidera el proyecto de implementación del SGSI. Este proyecto comenzó en junio de 2024 y se enfrenta a desafíos como la inclusión de empleados remotos y la consideración de los servidores en la nube como parte del alcance.

Table 1

Aspecto	**Descripción**
Nombre de la Organización	Empresa XYZ
Tipo de Servicios	Servicios web en la nube mediante software especializado
Ubicación	Oficinas principales en Cuenca y trabajo remoto
Infraestructura	Operación en la nube utilizando Microsoft Azure
Normativa	Implementación de ISO 27001 para gestión de seguridad de la información

Table 1. Descripción de la información.

2. Definición del Alcance del SGSI

Objetivo del SGSI

Establecer, implementar, mantener y mejorar continuamente un sistema de gestión para proteger la confidencialidad, integridad y disponibilidad de la información relevante para los servicios web ofrecidos por XYZ. Esto incluye la prevención de accesos no autorizados, la protección contra pérdidas de datos y la garantía de continuidad del negocio.

Límites del SGSI

El SGSI abarca todos los procesos relacionados con la provisión de servicios web en la nube, desde el desarrollo y gestión del software hasta el soporte a clientes.

Locaciones Físicas

- Oficinas centrales de XYZ en Cuenca.
- Hogares de los empleados que trabajan de manera remota.

Infraestructura Tecnológica

- Servidores alojados en Microsoft Azure.
- Equipos portátiles de los empleados utilizados para actividades laborales.
- Redes internas y externas utilizadas para la comunicación.

Table 2

Ámbito	**Detalles**
Locaciones Físicas	Oficinas principales en Cuenca y hogares de empleados remotos
Infraestructura Tecnológica	Servidores en Microsoft Azure, equipos portátiles, redes internas y externas

Table 2. Límites del SGSI.

3. Interesados Relevantes

Los interesados relevantes incluyen:

Table 3

Interesado	Rol/Interés
Clientes	Confían en la seguridad de los servicios proporcionados
Empleados	Responsable de cumplir con las políticas y procedimientos de seguridad
Proveedores	Microsoft Azure como socio clave en infraestructura
Auditores	Validar el cumplimiento de ISO 27001

Table 3. Interesados Relevantes.

4. Justificación del Alcance

La inclusión de empleados remotos en el alcance del SGSI es esencial, ya que manejan información sensible en su trabajo diario. Aunque no se puede garantizar el control físico de sus entornos de trabajo, XYZ ha implementado medidas de seguridad lógica, como el uso de VPN, autenticación multifactor y cifrado de datos, para mitigar los riesgos.

La infraestructura en la nube de Microsoft Azure también es parte integral del SGSI, dado que XYZ depende de esta plataforma para ofrecer sus servicios. Aunque XYZ no tiene control físico sobre los servidores, la certificación ISO 27001 de Azure proporciona un nivel adicional de garantía.

Table 4

Área	Justificación
Empleados remotos	Manejan información sensible; implementación de controles como VPN y cifrado.
Microsoft Azure	Dependencia crítica; certificación ISO 27001 asegura un nivel base de seguridad.

Table 4. Justificación del Alcance.

5. Identificación de Activos Clave

Table 5

Activo	Descripción
Software especializado	Herramienta principal para la provisión de servicios web
Datos de clientes	Información sensible y confidencial

Infraestructura Azure	Plataforma esencial para almacenamiento y procesamiento
Equipos portátiles	Dispositivos de trabajo utilizados por los empleados
Redes de comunicación	Infraestructura utilizada para transferir datos de forma segura
Políticas de seguridad	Lineamientos para la protección de la información

Table 5. Identificación de Activos Clave.

6. Consideraciones de Riesgo

Riesgo	Descripción
Accesos no autorizados	Posibilidad de comprometer sistemas sensibles
Pérdida de dispositivos	Riesgo de exposición de datos en equipos fuera del entorno controlado
Brechas en conexiones	Vulnerabilidades en redes de empleados remotos
Fallas de configuración	Errores que puedan exponer información sensible
Amenazas internas	Errores humanos o mal uso intencional de recursos

Table 6. Consideraciones de Riesgo

7. Roles y Responsabilidades

Table 7

Rol	Responsabilidad
CTO (Pablo)	Implementación y supervisión general del SGSI
Administrador de Sistemas	Gestión de infraestructura tecnológica y configuraciones
Equipo de Seguridad	Detección y respuesta ante incidentes
Empleados	Cumplimiento de políticas y procedimientos

Table 7. Consideraciones de Riesgo

8. Declaración de Aplicabilidad

La declaración de aplicabilidad incluye:

Control	Descripción
Control de accesos	Garantizar que solo personal autorizado acceda a información sensible
Cifrado de datos	Proteger datos en reposo y en tránsito mediante técnicas avanzadas
Auditorías periódicas	Revisiones constantes para asegurar cumplimiento de políticas
Capacitación	Entrenamiento a empleados sobre mejores prácticas de seguridad

Table 8. Declaración de Aplicabilidad

9. Exclusiones del Alcance

Table 9

Exclusión	Razón
Datos personales	No relacionados con la operación de servicios web
Equipos personales	No autorizados para actividades laborales

Table 9. Exclusiones del Alcance

10. Referencias

[1] “Entrar al sitio | aula,” Espe.edu.ec, 2025. https://micampus.espe.edu.ec/pluginfile.php/312348/mod_resource/content/1/Norma-ISO-27001-2022.pdf (accessed Jan. 14, 2025).