Sistema de Gestión de Seguridad de la Información (SGSI)

Universidad de California – Resumen Ejecutivo

Camila Aranibar Pozo

Tema ISO 27001

Introducción

El SGSI complementa las políticas IS-3 e ISMP de la Universidad.
Dado que el IS-3 Integra estándares ISO 27001, NIST 800-171, HIPAA y PCI-DSS, nos centraremos en añadir los controles CIS para tener un mayor enfoque.

Objetivo: mantener la confidencialidad, integridad y disponibilidad de la información de la universidad

Objetivo y alcance

Alcance: Toda la infraestructura TI, red, sistemas, campus, cloud y sedes

Objetivo:

Reducir y gestionar el ciberriesgo

Proteger la información y privacidad de los datos.

Fomentar cultura de ciberseguridad.

Evaluación de riesgos

Metodología

Análisis de activos, amenazas, vulnerabilidades, impacto y probabilidad.

Clasificación de riesgos: Alto, Medio, Bajo

Hallazgos

Alto riesgo en bases de datos, servidores, almacenamiento en la nube, ordenadores, copias de seguridad y Wi-Fi.

Controles recomendados

Controles CIS prioritarios a implementar de inmediato para mitigar riesgos críticos:

Control CIS	Descripción	Activos
CIS 4	Configuración segura de sistemas	Todos los activos críticos
CIS 6	Gestión de control de accesos	Bases de datos, apps, nube, carpetas
CIS 10	Defensas contra malware	PCs, servidores, OS
CIS 3	Protección de datos sensibles	Cloud, bases de datos, carpetas
CIS 12	Gestión de red y segmentación	Switches, firewalls
CIS 16	Seguridad en desarrollo y uso de software	Aplicaciones internas
CIS 11	Copias de seguridad y recuperación	Carpetas, bases de datos
CIS 5	Gestión de cuentas de usuarios	Móviles, PCs, cloud
CIS 8	Gestión de logs de auditoría	Todos

Plan de implementación

Corto plazo

En este periodo de máximo 3 meses se implementarán los controles CIS 4, CIS 6, CIS 10, CIS 3.

Medio plazo

En un periodo de 3 a 6 meses se implementarán los controles CIS 5, CIS 12, CIS 11, CIS 8

Largo plazo

Este peridod es de 6 a 12 meses, donde se implementarán los controles CIS 1, CIS 2, CIS 7, CIS 16, CIS 15, CIS 13, CIS 14

Políticas y Procedimientos

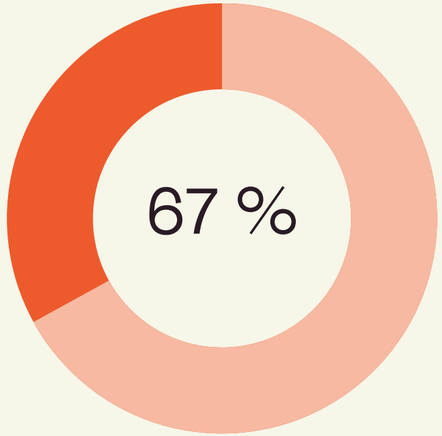
Se refuerza la documentación del IS-3

- Política de Seguridad
- Control de Acceso de Usuarios
- Plan de Respuesta a Incidentes
- Copia de Seguridad y Recuperación de Datos
- Concienciación y Capacitación de los Empleados
- Aprobación y Revisión de Documentos

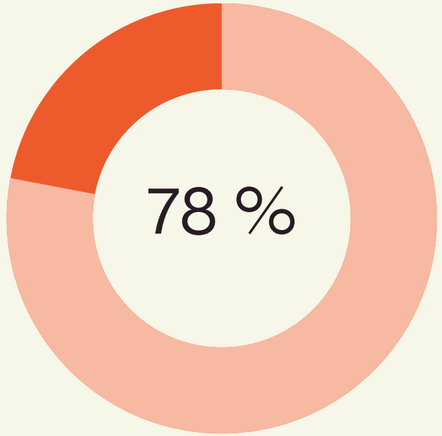
Próximos Pasos

- Aprobación del plan por dirección.
- Inicio de implementación de los controles por fases.
- Seguimiento de los controles, mejora continua y auditorías periódicas.

Estimación de las mejoras



Situación actual de la seguridad



Situación a final de año con la implementación con los controles

Gracias