Controles Anexo A ISO 27.001:2013

Introducción

Una buena manera de comprender el alcance e implicancias que tiene para una organización la implantación de una norma en seguridad de la información como lo es la ISO 27.001:2013, es revisando los controles que debe cumplir.

De esta forma es posible dimensionar y evaluar todos los temas y subtemas que deben ser parte de la gestión de la seguridad en las empresas.

Anexo A	Políticas de seguridad de la información	Orientación de administración para la seguridad de la información
A.5	Políticas de Seguridad de la Información	Orientación de administración para la Seguridad de la Información
A.6	Organización de la seguridad de la información	Organización Interna
		Dispositivos móviles y teletrabajo
A.7	Seguridad de Recursos Humanos	Antes del empleo
		Durante el empleo
		Despido y cambio de empleo
A.8	Administración de Activos	Responsabilidades por los activos
		Clasificación de la información
		Manejo de Medios
A.9	Control de acceso	Requisitos de negocio para el control de acceso
		Administración de acceso a los usuarios
		Responsabilidades de los usuarios
		Control de acceso de sistemas y aplicaciones
A.10	Criptografía	Controles criptográficos
A.11	Seguridad física y ambiental	Áreas seguras
		Equipos
A.12	Seguridad de las operaciones	Procedimientos y responsabilidades operacionales
		Protección contra malware
		Respaldo
		Registro y monitoreo
		Control software operacional
		Administración de vulnerabilidades técnicas
		Consideraciones sobre la auditoría de los sistemas de información
A.13	Seguridad en las comunicaciones	Administración de la seguridad de redes
		Transferencia de información
A.14	Adquisición, desarrollo y mantenimiento de sistemas	Requisitos de seguridad de los sistemas de información
		Seguridad en los procesos de desarrollo y soporte
		Datos de pruebas
A.15	Relaciones con los proveedores	Seguridad de la información en las relaciones con los proveedores
		Administración de prestación de servicios de proveedores

A.16	Administración de incidentes de seguridad de la información	Administración de incidentes y mejoras de seguridad en la información
A.17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Continuidad de la seguridad de la información
		Redundancias
A.18	Cumplimiento	Cumplimiento con los requisitos legales y contractuales
		Revisiones de la seguridad de la información

Durante el año 2022 se liberó la nueva versión ISO 27.001:2022 que incorpora controles nuevos, modifica algunos y elimina o combina otros. Es probable transcurra algún tiempo hasta que se comience a certificar en esta nueva versión, pero es conveniente tenerla presente.