CONTROLES ISO 27002:2022

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

5. CONTROLES ORGANIZACIONALES

CONTROL	NOMBRE
5.1	Políticas para la seguridad de la información
5.2	Roles y responsabilidades en seguridad de la información
5.3	Segregación de funciones
5.4	Responsabilidades de gestión
5.5	Contacto con autoridades
5.6	Contacto con grupos de interés especial
5.7	Inteligencia de Amenazas
5.8	Seguridad de la información en la gestión de proyectos
5.9	Inventario de información y otros activos asociados
5.10	Uso aceptable de la información y otros activos asociados
5.11	Devolución de activos
5.12	Clasificación de la información
5.13	Etiquetado de la información
5.14	Transferencia de la información
5.15	Control de acceso
5.16	Gestion de identidad
5.17	Informacion de autenticacion
5.18	Derechos de acceso
5.19	Seguridad de la información en las relaciones con los proveedores
5.20	Directrices de seguridad de la información en los acuerdos con proveedores
5.21	Gestión de la seguridad de la información en la cadena de suministro de TIC
5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores
5.23	Seguridad de la información para el uso de servicios en la nube
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información
5.25	Evaluación y decisión sobre los eventos de seguridad de información
5.26	Respuesta a incidentes de seguridad de la información
5.27	Aprendizaje de los incidentes de seguridad de la información
5.28	Recopilación de evidencias
5.29	Seguridad de la información durante interupciones
5.30	Preparación de las TIC para la continuidad del negocio
5.31	Identificación de requerimientos legales, estatutarios, regulatorios y contractuales
5.32	Derechos de Propiedad Intelectual (DPI)
5.33	Protección de registros
5.34	Privacidad y protección de PII
5.35	Revisión independiente de la seguridad de la información
5.36	Cumplimiento con políticas y estándares de seguridad de la información

6. CONTROLES DE PERSONAS

CONTROL	NOMBRE
6.1	Investigación de antecedentes
6.2	Términos y condiciones del empleo
6.3	Concientización, educación y capacitación en seguridad de la información
6.4	Proceso disciplinario
6.5	Responsabilidades ante la finalización o cambio
6.6	Acuerdos de confidencialidad o no revelación
6.7	Teletrabajo
6.8	Reporte de eventos de seguridad de la información

7. CONTROLES FÍSICOS

CONTROL	NOMBRE
7.1	Perímetro de seguridad física
7.2	Controles de entrada física
7.3	Seguridad de oficinas, despachos y recursos
7.4	Supervisión de la seguridad física
7.5	Protección contra las amenazas fisicas y ambientales
7.6	Trabajar en áreas seguras
7.7	Escritorio limpio y pantalla limpia
7.8	Ubicación y protección del equipo
7.9	Seguridad de los activos fuera de las instalaciones
7.10	Medios de almacenamiento
7.11	Utilidades de apoyo
7.12	Seguridad del cableado
7.13	Mantenimiento de los equipos
7.14	Eliminación segura o reutilización de equipos

8. CONTROLES TECNOLÓGICOS

CONTROL	NOMBRE
8.1	Dispositivos de punto final del usuario (End Point)
8.2	Derechos de acceso privilegiado
8.3	Restricción del acceso a la información
8.4	Acceso al código fuente
8.5	Autenticación segura
8.6	Gestión de la capacidad
8.7	Protección contra malware
8.8	Gestión de vulnerabilidades técnicas
8.9	Gestión de la configuración
8.10	Eliminación de la información
8.11	Enmascaramiento de datos
8.12	Prevención de la fuga de datos
8.13	Copias de seguridad de la información
8.14	Redundancia de las instalaciones de procesamiento de información
8.15	Gestión de eventos (Log)
8.16	Actividades de seguimiento
8.17	Sincronización del reloj
8.18	Uso de programas de utilidad privilegiados
8.19	Instalación de software en sistemas operativos
8.20	Controles de red
8.21	Seguridad de los servicios de red
8.22	Segregación en redes
8.23	Filtrado Web
8.24	Uso de Criptografía
8.25	Ciclo de vida de desarrollo seguro
8.26	Requisitos de seguridad en aplicaciones
8.27	Arquitectura del sistema seguro y principios de ingeniería
8.28	Codificación Segura
8.29	Pruebas de seguridad en el desarrollo y aceptación
8.30	Desarrollo subcontratado
8.31	Separación de los entornos de desarrollo, prueba y producción
8.32	Gestión del cambio
8.33	Información de prueba
8.34	Protección de sistemas de información durante pruebas de auditoría