ESCUELA DE POSTGRADO
Y EDUCACIÓN CONTINUA
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
UNIVERSIDAD DE CHILE

ISO 27001:2022

Referencia de controles de seguridad de la información en ISO 27001:2022 (Anexo A)

Alejandro González P.

6 Planificación

6.1 Acciones para abordar los riesgos y las oportunidades

6.1.3 Tratamiento de riesgo de la seguridad de la información

d) **generar una Declaración de Aplicabilidad** que contenga los controles necesarios [consultar 6.1.3 b) y c)], y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A;

AGo

Controles de Seguridad de la Información

La referencia de controles de seguridad de la información está enumerada desde el A.5 al A8, ello corresponde a las cláusulas 5 a 8 de ISO 27002:2022

ISO 27002:2022

- A cada control de ISO 27002 se le han asociado cinco atributos con sus correspondientes valores de atributo como sigue:

Tipo de control	Propiedades de SI	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo #Correctivo	#confidencialidad #integridad #disponibilidad	#identificar #proteger #detectar #responder #recuperar	#gobernanza #Gestión de activos #Information_protection #HR_security #Physical_security #System&network_security #Application_security #Secure_configuration #Identity_and_access_ Management #Threat_and_vulnerability_management #Continuit #Supplier_relationships_security #Legal_and_compliance #Information_security_event_management #Information_security_ assurance.	#Governance and Ecosystem #Protection #Defence #Resilience

AGo

Referencia de controles de seguridad de la información

AGo

5. Controles organizativos

5.1	Políticas de seguridad de la información	**Control** Política de seguridad de la información y políticas específicas de cada tema se deben definir, aprobadas por dirección, publicadas, comunicadas y reconocidas por personal y partes interesadas pertinentes, revisadas a intervalos planificados y si se producen cambios significativos.
5.2	Funciones y responsabilidades de seguridad de la información	**Control** Las funciones y responsabilidades de seguridad de la información se deben definir y asignar en función de necesidades de la organización.
5.3	Segregación de funciones	**Control** Funciones y áreas de responsabilidad conflictivas deben estar separadas.
5.4	Responsabilidades de gestión	**Control** La dirección debe exigir a todo personal que aplique seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos de la organización.
5.5	Contacto con autoridades	**Control** La organización debe establecer y mantener el contacto con las autoridades pertinentes.
5.6	Contacto con grupos de interés especial	**Control** La organización debe establecer y mantener contactos con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
5.7	Inteligencia de amenazas (nuevo control)	**Control** La información relacionada con las amenazas a la seguridad de la información se debe recopilar y analizar para generar inteligencia de amenazas.

AGo

5.8	Seguridad de información en gestión de proyectos	**Control** La seguridad de información se debe integrar en gestión del proyecto.
5.9	Inventario de información y otros activos asociados	**Control** Se debe elaborar y mantener un inventario de información y otros activos asociados, incluyendo propietarios.
5.10	Uso aceptable de información y otros activos asociados	**Control** Se debe identificar, documentar y aplicar normas para uso aceptable y procedimientos para el manejo de información y otros activos asociados.
5.11	Retorno de activos	**Control** Cuando corresponda, el personal y otras partes interesadas deben devolver todos los bienes de la organización que estén en su poder al cambiar o terminar su empleo contrato o acuerdo.
5.12	Clasificación de información	**Control** La Información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización, en función de la confidencialidad, integridad, disponibilidad y requisitos de partes interesadas.
5.13	Etiquetado de información	**Control** Se debe desarrollar y aplicar un conjunto adecuado de procedimientos para etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización.
5.14	Transferencia de información	**Control** Se deben establecer normas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización, entre la organización y otras partes.

5.15	Control de acceso	**Control** Las reglas para controlar el acceso físico y lógico a la información y a otros activos asociados se deben establecer y aplicar en función de los requisitos de seguridad de la empresa y de información.
5.16	Gestión de identidad	**Control** Se debe gestionar todo el ciclo de vida de las identidades.
5.17	Información de autenticación	**Control** La asignación y gestión de la información de autenticación se debe controlar por un proceso de gestión, que incluya asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
5.18	Derechos de acceso	**Control** Los derechos de acceso a la información y otros activos asociados se debe proporcionar, revisar, modificar y eliminar de acuerdo con la política específica de la organización sobre temas y reglas para el control de acceso.
5.19	Seguridad de la información en la relación con los proveedores	**Control** Se debe definir, aplicar procesos y procedimientos para gestionar riesgos de seguridad de la información asociados al uso de productos o servicios de proveedores.
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	**Control** Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación con el proveedor.
5.21	Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)	**Control** Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.

5.22	Monitoreo, revisión y gestión de cambios de servicios del proveedor	**Control** La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
5.23	Seguridad de la información para uso de servicios en la nube (nuevo control)	**Control** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización.
5.24	Planificación y preparación de gestión de incidentes de seguridad de la información	**Control** La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
5.25	Evaluación y decisión sobre eventos de seguridad de la información	**Control** La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	**Control** Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
5.27	Aprendizaje sobre incidentes de seguridad de la información	**Control** El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información.
5.28	Recolección de pruebas	**Control** La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

AGo

5.29	Seguridad de la información durante interrupción	**Control** La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante las interrupciones.
5.30	Preparación de TIC para continuidad de actividad (nuevo control)	**Control** La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
5.31	Requisitos legales, reglamentarios y contractuales	**Control** Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.
5.32	Derechos de propiedad intelectual	**Control** La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
5.33	Protección de registros	**Control** Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
5.34	Privacidad y protección de la información de identificación personal (PII)	**Control** La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.
5.35	Revisión independiente de seguridad de la información	Control El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

AGo

5.36	Cumplimiento de políticas, reglas y normas de seguridad de la información	**Control** El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos de cada tema se revisará periódicamente.
5.37	Procedimientos operativos documentados	**Control** Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

AGo

6. Controles de personas

6.1	Selección	**Control** Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y la riesgos percibidos.
6.2	Términos y condiciones del contrato de trabajo	**Control** Los acuerdos contractuales de trabajo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.
6.3	Concientización, educación y capacitación en seguridad de la información	**Control** El personal de la organización y las partes interesadas relevantes deben recibir la toma de conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.
6.4	Proceso disciplinario	**Control** Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
6.5	Responsabilidades tras el término o cambio de empleo	**Control** Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y otras partes interesadas.

6.6	Acuerdos de confidencialidad o no divulgación	**Control** Los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.
6.7	Trabajo a distancia	**Control** Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.
6.8	Informe de eventos de seguridad de la información	**Control** La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

AGo

7. Controles físicos

7.1	Perímetros de seguridad física	**Control** Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.
7.2	Acceso físico	**Control** Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.
7.3	Asegurar oficinas, salas e instalaciones	**Control** Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.
7.4	Supervisión de seguridad física (nuevo control)	**Control** Las instalaciones deben estar vigiladas continuamente para evitar acceso físico no autorizado.
7.5	Protección contra amenazas físicas y medioambientales	**Control** Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
7.6	Trabajo en zonas seguras	**Control** Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.
7.7	Escritorio y pantalla despejados	**Control** Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.

7.8	Emplazamiento y protección de equipos	**Control** El equipo se colocará de forma segura y protegida.
7.9	Seguridad de los activos fuera de las instalaciones	**Control** Se protegerán los activos fuera de las instalaciones.
7.10	Medios de almacenamiento	**Control** Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
7.11	Servicios de apoyo	**Control** Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
7.12	Seguridad del cableado	**Control** Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.
7.13	Mantenimiento de equipos	**Control** Los equipo se mantendrán correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.
7.14	Eliminación segura o reutilización de equipos	**Control** Los equipos que contienen soportes de almacenamiento se deben verificar para garantizar que cualquier dato sensible y “software” con licencia se eliminó o sobrescribió de forma segura antes de su eliminación o reutilización.

AGo

8. Controles tecnológicos

8.1	Dispositivos terminales de usuario	**Control** Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.
8.2	Derechos de acceso privilegiado	**Control** La asignación y uso de derechos de acceso privilegiados se debe restringir y gestionar.
8.3	Restricción de acceso a la información	**Control** El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.
8.4	Acceso a código fuente	**Control** El acceso de lectura y escritura a código fuente, a herramientas de desarrollo y a bibliotecas de "software" debe ser gestionado adecuadamente.
8.5	Autenticación segura	**Control** Las tecnologías y procedimientos de autenticación segura deben ser aplicadas en función de las restricciones de acceso a la información y de las políticas específicas de control de acceso.
8.6	Gestión de la capacidad	**Control** La utilización de los recursos debe supervisarse y ajustarse de conformidad con las necesidades de capacidad actuales y previstas.
8.7	Protección contra "malware"	**Control** La protección contra el malware debe implementarse y respaldarse con el conocimiento adecuado del usuario.

AGo

8.8	Gestión de vulnerabilidades técnicas	**Control** Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
8.9	Gestión de configuración (nuevo control)	**Control** Las configuraciones, incluyendo las configuraciones de seguridad, de "hardware", "software", servicios y redes se deben establecer, documentar, aplicar, supervisar y revisar.
8.10	Supresión de información (nuevo control)	**Control** La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesaria.
8.11	Enmascaramiento de datos (nuevo control)	**Control** El enmascaramiento de datos se debe usar de acuerdo con la política específica de la organización sobre control de acceso y otras políticas específicas relacionadas con el tema, así como con los requisitos empresariales, teniendo en cuenta la legislación aplicable.
8.12	Prevención de fuga de datos (nuevo control)	**Control** Las medidas de prevención de fuga de datos se deben aplicar a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
8.13	Respaldo de información	Las copias de seguridad de la información, de "software" y de sistemas se deben mantener y probar periódicamente de acuerdo con la política específica acordada sobre copias de seguridad.
8.14	Redundancia de instalaciones de tratamiento de información	**Control** Las instalaciones de procesamiento de información se debe implementar con la redundancia suficiente para cumplir con requisitos de disponibilidad.

AGo

8.15	Inicio de sesión	**Control** Se debe producir, almacenar, proteger y analizar registros que graben actividades, excepciones, fallos y otros eventos relevantes.
8.16	Actividades de monitoreo (nuevo control)	**Control** Las redes, sistemas y aplicaciones se deben supervisar para detectar comportamientos anómalos y tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.
8.17	Sincronización de reloj	**Control** Los relojes de los sistemas de procesamiento de la información usados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas.
8.18	Uso de programas utilitarios privilegiados	**Control** El uso de programas utilitarios que pueden ser capaces de anular los controles de sistema y de aplicación se deben restringir y controlar estrictamente.
8.19	Instalación de “software” en sistemas operativos	**Control** Se debe aplicar procedimientos y medidas para gestionar de forma segura la instalación de “software” en los sistemas operativos.
8.20	Seguridad de redes	**Control** Las redes y dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de sistemas y aplicaciones.
8.21	Seguridad de servicios de red	**Control** Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red se deben identificar, implementar y supervisar.
8.22	Segregación de redes	**Control** Grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.

AGo

8.23	Filtrado web (nuevo control)	**Control** El acceso a sitios Web externos se debe gestionar para reducir exposición a contenidos maliciosos.
8.24	Uso de criptografía	**Control** Se deben definir y aplicar normas para uso eficaz de la criptografía, incluida gestión de claves criptográficas.
8.25	Ciclo de vida de desarrollo seguro	**Control** Se deben establecer y aplicar normas para desarrollo seguro de "software" y sistemas.
8.26	Requisitos de Seguridad de las aplicaciones	**Control** Los requisitos de seguridad de información se deberían identificar, especificar y aprobar en que desarrollar o adquirir aplicaciones.
8.27	Principios de ingeniería y arquitectura de sistemas seguros	**Control** Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicar a cualquier actividad de desarrollo de sistemas de información.
8.28	Codificación segura (nuevo control)	**Control** Se debe aplicar principios de codificación segura al desarrollo de "software".
8.29	Pruebas de seguridad en desarrollo y aceptación	**Control** Los procesos de pruebas de seguridad se deben definir e implementar en el ciclo de vida de desarrollo.
8.30	Desarrollo externalizado	**Control** **La** organización debe dirigir, supervisar y revisar las actividades relacionadas con desarrollo de sistemas subcontratados.

AGo

8.31	Separación de entornos de desarrollo, prueba y producción	**Control** Los entornos de desarrollo, pruebas y producción deben estar separados y asegurados.
8.32	Gestión de cambio	**Control** Los cambios en instalaciones de procesamiento de información y en sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
8.33	Información de prueba	**Control** La información de usada en las pruebas se debe seleccionar, proteger y gestionar adecuadamente.
8.34	Protección de sistemas de información durante pruebas de auditoría	**Control** Las pruebas de auditoría y otras actividades de garantía que impliquen evaluación de sistemas operativos se deben planificar y acordar entre el encargado de pruebas y la dirección correspondiente.

AGo

ESCUELA DE POSTGRADO
Y EDUCACIÓN CONTINUA
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
UNIVERSIDAD DE CHILE

ISO 27001:2022

Referencia de controles de seguridad de la información en ISO 27001:2022 (Anexo A)

Alejandro González P.