agesic

Uruguay **Presidencia**

GUÍA DE IMPLEMENTACIÓN

Marco de referencia

SEGURIDAD DE LA INFORMACIÓN

Versión 4.1 – Noviembre 2019

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tenga en cuenta citar la obra de forma específica.

1 Revisiones

Versión 1.0 (agosto 2016):

a. Versión inicial

Versión 2.0 (noviembre 2016):

a. Se realizan cambios menores de redacción.

Versión 3.0 (junio 2017):

a. Se realiza cambio de enfoque respecto al modelo de madurez propuesto en la versión 1.0

Versión 4.0 (enero 2018):

a. Se agrega, para cada requisito, una contextualización propia para instituciones de salud.

b. Se mejora redacción de cómo implementar cada requisito.

c. Se agregan términos al glosario y definiciones.

d. Se elimina el requisito SO.1 “Documentar los procedimientos de operación” por estar contemplado en diversos requisitos.

e. El requisito SO.9 “Gestionar las vulnerabilidades técnicas” pasa a tener el código SO.1

f. Se mejoran los nombres de los requisitos, sin que esto impacte en su alcance u objetivo. Los más significativos son:

   i. El requisito CO.6 “Definir los mecanismos de comunicación e interlocutores válidos para la comunicación con la prensa” pasa a llamarse “Definir los mecanismos de comunicación e interlocutores válidos”.

   ii. El requisito GA.5 “Destrucción de información y medios de almacenamiento” pasa a llamarse “Establecer los mecanismos para destruir la información y medios de almacenamiento”.

   iii. El requisito SC.12 “De implementar servicios de Webmail estos deben ser implementados sobre el protocolo HTTPS utilizando un certificado de seguridad válido, y deberán estar alojados dentro del territorio nacional. Los titulares de cuentas de correo de dominios gubernamentales no podrán acceder a sus cuentas desde servicios Webmail que no sean el provisto por el organismo. Cuando la información a transmitir vía email represente un riesgo alto para el organismo se recomienda implementar un modelo de cifrado a nivel de mensaje” pasa a llamarse “De implementar servicios de Webmail estos deben ser implementados sobre el protocolo HTTPS utilizando un certificado de seguridad válido. Cuando la información a

transmitir vía email represente un riesgo alto para la organización se recomienda implementar un modelo de cifrado a nivel de mensaje".

iv. El requisito SO.7 "Registrar los eventos de los sistemas" pasa a llamarse "Registrar y monitorear los eventos de los sistemas".

Versión 4.1 (noviembre 2019):

a. El punto 4.1 Gestión de Riesgo fue modificado. El requisito GR.1 se divide en los requisitos GR.1 GR.2 y GR.3.

b. El punto 4.2 Planificación fue modificado y se agregó el requisito PL.2.

c. Se mejoró la redacción del requisito GI.6.

d. Se realizaron adecuaciones en algunos requisitos en la guía de implementación y guía de auditoria a fin de mejor su implementación y verificación.

2 Introducción

Los requisitos de esta Guía se encuentran asociados a las subcategorías del Marco de Ciberseguridad. La guía de requisitos se ha implementado tomando como base las categorías de control definidas en las normas UNIT-ISO/IEC 27001:2013 y UNIT-ISO/IEC 27002:2013 (Adopción UNIT Noviembre 2014, Edición corregida 2015-12-15), así como la normativa vigente referida a seguridad de la información.

Los requisitos detallados a continuación son los que al leal saber y entender de Agesic, es necesario implementar para lograr fortalecer la gestión de seguridad de la información, en alineación con la normativa vigente y mejores prácticas internacionales en la materia. Agesic no será responsable por la identificación y/o definición de las políticas y procedimientos específicos de cada organización que puedan derivar de cada requisito y/o de las guías de implementación. Este documento es una guía de requisitos e implementación de controles. Agesic no será responsable por no identificar mejoras de procesos respecto a la gestión de la seguridad de la información en las organizaciones. Todas las decisiones sobre la gestión de la seguridad de la información y en particular la aplicación de esta guía serán responsabilidad de cada organización.

3 Objetivo y alcance

Los objetivos específicos son:

- Establecer los requisitos mínimos necesarios para implantar un Sistema de Gestión de Seguridad de la Información.
- Explicar el objetivo de cada uno de los requisitos.
- Establecer una referencia a las mejores prácticas internacionales de gestión de seguridad de la información.
- Brindar una guía de implementación basada en las mejores prácticas internacionales.
- Proveer documentación de apoyo que pueda ser reutilizada y adaptada por cada organización para implementar los requisitos.

4 Requisitos

Interpretación de la tabla donde se presenta cada uno de los requisitos.

Requisito XX.N	Descripción de lo que la organización debe cumplir en función de la normativa vigente relacionada a la seguridad de la información y las buenas prácticas en la materia.
Objetivo	Describe qué es lo que se desea lograr mediante la implementación del requisito.
Alcance	Determina los tipos de organizaciones que deben adoptar el requisito. Cuando refiere a “Administración Central” únicamente es porque está asociado a un decreto o normativa específica. Se debe tener en cuenta que en estos casos también se exhorta su cumplimiento al resto de los organismos del Estado, servicios descentralizados y entes autónomos.
Referencia ISO 27001:2013	Control o conjunto de controles de la norma ISO 27001:2013 asociado total o parcialmente.
Guía de implementación	Sugerencias, mejores prácticas y/o guías metodológicas para lograr alcanzar el objetivo y, por consiguiente, implementar el requisito.
Administración Central	Aspectos específicos aplicables a la realidad de Administración Central.
Instituciones de salud	Aspectos específicos aplicables a la realidad de las instituciones de salud.
Guía de evidencia para auditoría	Se detalla una lista de evidencias a modo de guía para las organizaciones. La lista no es exhaustiva, su finalidad es servir de apoyo o guía a las organizaciones y proveedores para verificar la implementación de los requisitos detallados en el presente marco. Esta lista no garantiza que las organizaciones no tengan observaciones de mejora.
Normativa asociada	Ley, decreto o resolución que menciona expresamente el cumplimiento del mencionado requisito.
Documentación de apoyo asociada	Anexo o documentación que colabora a la implementación del requisito.

4.1 Gestión de riesgos

Requisito GR.1	Adoptar una metodología de Evaluación de Riesgo alineada a las necesidades del SGSI.
Objetivo	Establecer un proceso de evaluación de riesgo en base a una metodología que permita guiar a la organización por las buenas prácticas de la evaluación del riesgo a nivel tecnológico y de procesos; permitiendo establecer su apetito riesgo, la tolerancia sobre las desviaciones, calcular la probabilidad de ocurrencias y el impacto potencial sobre la materialización de las vulnerabilidades.
Alcance	Cualquier organización.
Referencia ISO 27001	Cláusulas 6.1.1, 6.1.2, 6.1.3, 8.2, 8.3
Guía de implementación	Se debe adoptar una metodología de evaluación de riesgo basado en la identificación de amenazas y vulnerabilidades, que pueda aplicarse a todos los aspectos tecnológicos, y que esté alineada a la gestión de riesgos de negocio de la organización. <u>Política</u> Se debe definir una política de gestión de riesgos de seguridad de la información basada en una metodología de gestión de riesgos y definir el responsable de su gestión. <u>Responsable</u> Si bien se debería definir un responsable para la gestión de riesgos, en un principio este rol puede coincidir con el del RSI. <u>Aprobación y difusión</u> La Política de Evaluación de Riesgo debe ser o formar parte de la adopción de la política de Seguridad de la Información la cual debe ser aprobada por la Dirección o CSI.
Administración Central	-
Instituciones de salud	Se debe realizar una evaluación de los posibles riesgos y vulnerabilidades a la confidencialidad, integridad y disponibilidad de la Historia Clínica Electrónica (HCE). Además, se debe realizar una evaluación de riesgos con relación a la conectividad de dispositivos médicos, contemplando: identificación de activos, identificación de tipo de conectividad, casos de uso, flujos de comunicación, exposición de servicios a Internet, segregación/segmentación para ubicar estos activos, control de acceso a los dispositivos y a la red, acceso remoto, cifrado de comunicación en tránsito, uso de certificados, gestión, operación y monitoreo de los dispositivos, hardening, etc.
Guía de evidencia para auditoría	• Metodología de gestión de riesgos de seguridad de la información (identificación, evaluación, tratamiento, seguimiento y comunicación a los interesados).

	• Política de gestión de riesgos de seguridad de la información. • Entrevistas al personal para corroborar el conocimiento de la Política de Evaluación de Riesgo. • Registro de cambios a la Política de Evaluación de Riesgo.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	Anexo I - AI.21 Política de Gestión de riesgos de seguridad de la información. Anexo III - AIII.9 Guía de equipo responsable de la gestión de riesgo.
Requisito GR.2	Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.
Objetivo	Contribuir al cumplimiento de los objetivos de seguridad de la información, prevenir o reducir los efectos no deseados y lograr la mejora continua.
Alcance	Cualquier organización.
Referencia ISO 27001	Cláusulas 6.1.1, 6.1.2, 6.1.3, 8.2, 8.3
Guía de implementación	Evaluación de riesgos De acuerdo a lo definido en el proceso de evaluación de riesgos de seguridad, se debe: • Establecer el alcance. • Identificar y documentar las amenazas y vulnerabilidades. • Identificar el impacto en el negocio en caso de materializarse los riesgos. • Identificar los controles necesarios para respuesta y mitigación, además de las medidas de seguridad ya implementadas. • Clasificar y monitorear los riesgos. • Establecer la periodicidad de las evaluaciones. Las principales tareas con relación a la evaluación de riesgos están referenciadas en la “Guía metodológica – Implantación SGSI” e “Inventario de activos y Evaluación de riesgos” (ver anexos).
Administración Central	-
Instituciones de salud	Se debe realizar una evaluación de los posibles riesgos y vulnerabilidades a la confidencialidad, integridad y disponibilidad de la Historia Clínica Electrónica (HCE). Además, se debe realizar una evaluación de riesgos con relación a la conectividad de dispositivos médicos, contemplando: identificación de activos, identificación de tipo de conectividad, casos de uso, flujos de comunicación, exposición de servicios a Internet, segregación/segmentación para ubicar estos activos, control de acceso a los dispositivos y a la red, acceso remoto, cifrado de comunicación en tránsito, uso de certificados, gestión, operación y monitoreo de los dispositivos, hardening, etc.

Guía de evidencia para auditoría	• Inventario de riesgos identificados y seguimiento para el período auditado. • Evaluación y/o análisis de riesgos. • Evaluación de proveedores.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	Anexo IV - AIV.1 Guía metodológica - implantación SGSI. Anexo IV - AIV.2 Inventario de activos y Evaluación de riesgos.
Requisito GR.3	Tratamiento o un plan de acción correctivo sobre los riesgos encontrados y, de acuerdo a su resultado, implementar las acciones correctivas y preventivas correspondientes.
Objetivo	Establecer un cronograma y plan de acción para mitigar los riesgos a corto y mediano plazo que se consideren inaceptables según la tolerancia al riesgo definida por la organización. Adicionalmente verificar que, una vez subsanados los riesgos con la aplicación de controles adicionales o compensatorios, los mismos se reducen a un nivel aceptable de exposición en relación a los efectos no deseados.
Alcance	Cualquier organización.
Referencia ISO 27001	Cláusulas 6.1.1, 6.1.2, 6.1.3, 8.2, 8.3
Guía de implementación	Tratamiento del riesgo De acuerdo a lo definido en el proceso tratamiento de riesgos de seguridad, se debe: • Elaborar un plan de acción de gestión de los riesgos. • Implementar las acciones correctivas y/o preventivas en los casos que corresponda. • Actualizar el plan de acción de gestión de riesgos. El resultado final de este análisis debe ser una lista priorizada de áreas de alto riesgo y una estrategia de control general para minimizar el riesgo para la organización en términos de impacto general.
Administración Central	-
Instituciones de salud	Se debe realizar una evaluación de los posibles riesgos y vulnerabilidades a la confidencialidad, integridad y disponibilidad de la Historia Clínica Electrónica (HCE). Además, se debe realizar una evaluación de riesgos con relación a la conectividad de dispositivos médicos, contemplando: identificación de activos, identificación de tipo de conectividad, casos de uso, flujos de comunicación, exposición de servicios a Internet, segregación/segmentación para ubicar estos activos, control de acceso a los dispositivos y a la red, acceso remoto, cifrado de comunicación en tránsito, uso de certificados, gestión, operación y monitoreo de los dispositivos, hardening, etc.

Guía de evidencia para auditoría	• Plan de tratamiento de riesgos incluyendo al menos, orden de prioridad y plazos de implementación de los controles identificados para tratar los riesgos. • Certificaciones funcionales y técnicas de las pruebas realizadas en los ambientes de test o calidad de que las vulnerabilidades han sido mitigadas. • Aprobaciones de los controles de cambio para las correcciones en los ambientes de producción. • Informe de re evaluación de mitigación o control de las vulnerabilidades.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	N/A

4.2 Planificación

Requisito PL.1	Establecer objetivos anuales con relación a la Seguridad de la Información.
Objetivo	Establecer la estrategia de seguridad de la información mediante objetivos claros en plazos anuales, alineados a la estrategia de la organización.
Alcance	Cualquier organización.
Referencia ISO 27001	Cláusula 6.2
Guía de implementación	Estrategia y objetivos Se debería establecer una estrategia de ciberseguridad y seguridad de la información alineada a la estrategia de la organización. La Dirección debe proporcionar lineamientos claros y un apoyo de gestión visible para las iniciativas de seguridad de la información dentro de la organización. Se deben establecer objetivos de seguridad de la información, al menos anualmente, a nivel de la organización. Estos objetivos pueden estar asociados a la adopción del marco de ciberseguridad, implementar nuevos requisitos y/o avanzar en el modelo de madurez. Los objetivos deberán organizarse en un plan de acción. Es recomendable que los lineamientos y objetivos vinculados a seguridad de la información sean planteados por el Comité de Seguridad de la Información (CSI) y sean difundidos a las partes interesadas. Del plan de acción deberían derivar proyectos concretos de seguridad de la información. Se pueden establecer indicadores para el seguimiento del cumplimiento de los objetivos planteados.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Listado de objetivos anuales de la organización relacionados con seguridad de la información. • Plan de acción.

	• Proyectos de seguridad de la información. • Estrategia de ciberseguridad y seguridad de la información. • Indicadores de seguimiento.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	Anexo IV - AIV.3 Indicadores SGSI Anexo V - Plan de acción
Requisito PL.2	Revisión periódica y mejora continua del SGSI
Objetivo	La organización debe garantizar la mejora de la estrategia, políticas, procedimientos y controles que se hayan adoptado para adecuarse a los cambios organizacionales y/o de contexto que haya tenido o pueda afrontar el negocio.
Alcance	Cualquier organización
Referencia ISO 27001	N/A
Guía de implementación	Para el cumplimiento del requisito, la Dirección debe: • Elaborar un Plan de acción anual que permita evaluar los cambios según criterios de calidad y nuevas características o acciones correctivas que requiera la organización. • Revisar los controles implementados y la documentación que los soporta. • Proveer las herramientas y entrenamientos necesarios al personal encargado de realizar las actividades, teniendo en cuenta su rol dentro de la organización. • Establecer los indicadores de medición y los resultados esperados a fin validar la calidad de las mejoras sugeridas. • Prueba de validación de que las mejoras realizadas cumplen con el objetivo pautados.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Plan de acción para la revisión de controles, procesos, estrategias y políticas. • Análisis de riesgos asociados a la mejora continua. • Establecimiento de tabuladores o indicadores de seguimiento y de mejora.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo IV - AIV.3 Indicadores de un SGSI.

4.3 Política de Seguridad de la Información

Requisito PS.1	Adoptar una Política de Seguridad de la Información.
Objetivo	Proporcionar lineamientos de gestión en línea acorde a los objetivos de la organización, contemplando la normativa aplicable. Disponer de medidas para garantizar la confianza y seguridad de los sistemas y de la información en poder de la organización, así como proteger los activos de información y minimizar el impacto en los servicios causados por amenazas o incidentes de seguridad. Demostrar el compromiso de la Dirección con la seguridad de la información.
Alcance	Cualquier organización
Referencia ISO 27001	A.5.1.1, A.5.1.2 y Cláusula 5.2
Guía de implementación	<u>Política de Seguridad de la Información</u> La Política de Seguridad de la Información debe estar respaldada por una planificación estratégica o plan de acción con roles y responsabilidades definidos para las diferentes funciones. <u>Aprobación y difusión</u> La Política de Seguridad de la Información debe ser aprobada por la Dirección o CSI y comunicada a todo el personal y terceras partes relevantes. <u>Revisión</u> La Política de seguridad de la información y demás políticas relacionadas, deben revisarse a intervalos regulares o cuando se produzcan cambios significativos para garantizar su adecuación y eficacia. Se deben definir indicadores para la medición de la efectividad de las políticas de seguridad definidas.
Administración Central	-
Instituciones de salud	La Política de Seguridad de la Información debe brindar las mayores garantías para salvaguardar la integridad, confidencialidad y disponibilidad de las historias clínicas, velando por la privacidad de la información sensible que está en poder de la institución.
Guía de evidencia para auditoría	• Resolución con la adopción de la Política de Seguridad de la Información. • Acceso a la publicación de la Política de Seguridad de la Información (por ejemplo, sitio institucional, Intranet, otros) y evidencia de su difusión. • Entrevistas al personal para corroborar el conocimiento de la Política de Seguridad de la Información. • Evidencia de revisión de la Política de Seguridad de la Información por parte de la Dirección (minutas, actas, correos, formularios, otros). • Registro de cambios a la Política de Seguridad de la Información.
Normativa asociada	Decreto 452/009 - Anexo I
Documentación de apoyo asociada	Anexo I - AI.1 Política de Seguridad de la Información para organismos de la Administración Central.

	Anexo I – AI.29 Política de Seguridad de la Información para instituciones de salud. Anexo II - AII.1 Resolución para la adopción de política, designación del RSI y conformación del CSI.

4.4 Organización y Gobernanza

Requisito OR.1	Designar un Responsable de la Seguridad de la Información.
Objetivo	Lograr liderazgo y guía en la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.
Alcance	Cualquier organización
Referencia ISO 27001	A.6.1.1 y Cláusula 5.3
Guía de implementación	Responsable de la Seguridad de la Información La organización debe designar a un Responsable de la Seguridad de la Información que desarrolle sus actividades en forma independiente de las áreas de tecnología. El RSI debe ser un referente de la temática en la organización y debe participar en la gestión de incidentes y la gestión de riesgos de seguridad. Se deben alinear las responsabilidades de seguridad de la información con las políticas de seguridad de la información que se encuentren definidas. Características del rol de RSI La persona designada para este rol debe contar con disponibilidad para cumplir adecuadamente con las funciones asignadas, así como también reportar directamente a la dirección de la organización. Liderazgo, capacidad para lograr acuerdos, aceptación de sus pares, conocimiento de riesgos, amenazas y vulnerabilidades de los activos; así como poder de gestión, son cualidades fundamentales para llevar con éxito la tarea de Responsable de la Seguridad de la Información. Se entiende necesario determinar la dedicación que debe tener quien asuma el rol en la organización.
Administración Central	El RSI debe participar de las reuniones de coordinación, periódicas, de los Responsables de Seguridad de la Información de su inciso. En caso de ser el RSI del inciso, éste debe coordinarlas. El RSI o quien éste determine, debe ser el punto de contacto con el CERTuy.
Instituciones de salud	Al momento de la firma del “Compromiso de uso adecuado de la Red Salud”, las instituciones deben indicar el contacto técnico y el RSI. El RSI o quien éste determine, debe ser el punto de contacto con el equipo de respuesta que corresponda.
Guía de evidencia para auditoría	• Designación de la función o rol de Responsable de la Seguridad de la Información.

	• Difusión de la designación del rol o función de Responsable de la Seguridad de la Información.
Normativa asociada	Decreto 452/009 (aplica para los organismos pertenecientes a la AC). Compromiso de uso adecuado de la Red Salud.
Documentación de apoyo asociada	Anexo II - AII.1 Resolución para la adopción de política, designación del RSI y conformación del CSI. Anexo III - AIII.1 Actividades del Responsable de la Seguridad de la Información. (Aplica para los organismos pertenecientes a la AC; no obstante, esta documentación de apoyo puede ser adaptada, tomada como base y/o utilizada por cualquier organización).
Requisito OR.2	Conformar un Comité de Seguridad de la Información.
Objetivo	Contar con un equipo de personas con capacidad de decisión sobre los objetivos de la organización, que vele por la seguridad de la información, marque los lineamientos estratégicos en la materia y defina los objetivos anuales.
Alcance	Cualquier organización
Referencia ISO 27001	A.6.1.1, A.6.1.3 y Cláusula 5.3
Guía de implementación	<u>Comité de Seguridad de la Información</u> Se debe designar los integrantes del Comité de Seguridad de la Información (CSI). El CSI debe estar formado por representantes de todas las direcciones o gerencias de la organización incluyendo responsable de TI. <u>Conformación</u> En términos generales, su conformación refiere a directivos con toma de decisiones dentro de la organización. <u>Funcionamiento</u> El CSI se debe reunir periódicamente. Cuando el CSI se reúna con el propósito de revisar temas referentes a la evaluación y tratamiento del riesgo de seguridad de la información, se debe incluir la participación del responsable de la Gestión de Riesgos. El CSI puede convocar a sus reuniones a otros expertos que considere pertinentes para el cumplimiento de sus cometidos. <u>Cometidos</u> Dentro de los principales cometidos del CSI se encuentran: • Establecer y aprobar sus pautas de funcionamiento. • Promover, difundir y apoyar la seguridad de la información, garantizando que sea parte de los procesos de planificación. • Definir las estrategias de seguridad de la información transversales a la organización. • Aprobar los planes, políticas y todo aquello que incremente y mejore la seguridad de la información.

	• Dar cuenta a la Dirección de la organización respecto a la no aprobación y/o no cumplimiento de las decisiones adoptadas por el referido Comité. • Establecer los niveles aceptables de riesgo.
Administración Central	El CSI debe estar formado por un equipo de personas con capacidad de decisión sobre los objetivos del organismo o inciso (según corresponda su alcance). Si el organismo pertenece a la Administración Central y el CSI está formado a nivel del inciso, su conformación es con los directores de las unidades ejecutoras. Si está formado a nivel de unidad ejecutora, se conforma con los directores de área. Dependiendo de la realidad y tamaño del organismo, los cometidos del CSI podrían incluirse a otros grupos ya existentes como el "Gabinete ministerial".
Instituciones de salud	Además de lo planteado en términos generales, el CSI debe contar con al menos un miembro perteneciente al área asistencial.
Guía de evidencia para auditoría	• Resolución de la creación del CSI. • Responsabilidades del CSI aprobados por la Dirección. • Pautas de funcionamiento del CSI. • Evidencia de las reuniones mantenidas por el CSI durante el período auditado (actas, orden del día, correos, otros).
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo II - AII.1 Resolución para la adopción de política, designación del RSI y conformación del CSI. Anexo II - AII.6 Pautas de funcionamiento del CSI.
Requisito OR.3	**Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.**
Objetivo	Contribuir con las buenas prácticas de gestión y control del SGSI dentro de la organización definiendo un procedimiento documentado de contacto con autoridades (internas y externas), ante un incidente de seguridad de la información y, particularmente, ante un incidente de seguridad informática.
Alcance	Cualquier organización
Referencia ISO 27001	A.6.1.3, A.6.1.4 y Cláusula 7.4
Guía de implementación	Procedimiento o plan de comunicación Se debe definir el procedimiento o plan de comunicación con autoridades tanto internas como externas en el caso de detectarse un incidente de seguridad de la información o eventos anómalos (confirmados o sospechados). El RSI o quien éste determine, debe ser el punto de contacto ante incidentes de seguridad de la información. Además, deben indicarse los medios por los cuales se puede o debe realizar el contacto; cómo se dejará constancia de las comunicaciones realizadas y cómo se realizará el seguimiento de cada incidente. La lista de contactos debe ser revisada a intervalos regulares para garantizar su adecuación. El procedimiento o plan debe contar con los pasos a seguir e identificar los contactos a los cuales informar.

	Relacionamiento con el equipo de respuesta ante incidentes Dicho procedimiento debe indicar cómo contactar con el equipo de respuestas ante incidentes de seguridad o a referentes con capacidad de articular soluciones, dependiendo del caso.
Administración Central	Dicho procedimiento debe definir específicamente en qué casos contactar al CERTuy (responsables, canales de comunicación, difusión del procedimiento). El CERTuy puede ser contactado a través de las vías de comunicación detalladas en su sitio Web. Es recomendable que el RSI mantenga contacto con CERTuy, foros y otros grupos especializados para estar atento al surgimiento de nuevas amenazas y vulnerabilidades.
Instituciones de salud	Ante incidentes de seguridad que afecten o puedan afectar a la infraestructura de HCEN (por ejemplo, incidentes en sistemas que procesan o almacenan información de salud) o sus sistemas circundantes (por ejemplo, servidores DNS, Firewalls, Correo, etc.), deben reportarse siempre al CERTuy o equipo de respuesta que corresponda.
Guía de evidencia para auditoría	• Plan de comunicación ante incidentes de seguridad de la información o crisis. • Plan de gestión de incidentes de seguridad de la información. • Evidencia de haber realizado el contacto con autoridades de acuerdo a los planes y procedimientos definidos para los incidentes (o potenciales incidentes) de seguridad de la información que se registraron en el período auditado. • Evidencias de incidentes o sospechas de seguridad reportados al CERTuy.
Normativa asociada	Decreto 451/009 Decreto 452/009
Documentación de apoyo asociada	Anexo I - AI.2 Política de Gestión de incidentes de seguridad de la información. Anexo III - AIII.2 Guía de actividades del responsable por la gestión de incidentes de seguridad de la información. Anexo III - AIII.4 Guía de procesos en gestión de incidentes.
Requisito OR.4	Abordar la seguridad de la información en la gestión de los proyectos.
Objetivo	Lograr que los temas relativos a seguridad de la información estén incluidos en todos los proyectos desde su inicio, independientemente del tipo de proyecto tratado.
Alcance	Cualquier organización
Referencia ISO 27001	A.6.1.5
Guía de implementación	Se deben incluir requerimientos de seguridad de la información dentro de los requerimientos de los proyectos, por ejemplo, en el acta de constitución del proyecto. En la evaluación de riesgos del proyecto deben incluirse riesgos de seguridad de la información.
Administración Central	-

Instituciones de salud	Todo proyecto que incluya dispositivos médicos con conectividad debe tener una evaluación de riesgos específica, y contemplar requisitos de ciberseguridad dentro de la gestión del proyecto. En particular, considerar proyectos relacionados a sistemas que interactúan con la plataforma HCEN, como: HIS, LIS, RIS, PACS, entre otros.
Guía de evidencia para auditoría	• Lista de proyectos llevados a cabo o en proceso durante el período a auditar. • Documentación de los proyectos (por ejemplo, acta de constitución del proyecto, lista inicial de requerimientos, etc.) que incluya requisitos de seguridad de la información requeridos. • Evidencia de realización y seguimiento de la evaluación de riesgos de los proyectos que incluyan riesgos relativos a la seguridad de la información. • Informes de avance de los proyectos donde se incluye puntos que tratan sobre la evaluación de los riesgos de seguridad de la información.
Normativa asociada	N/A
Documentación de apoyo asociada	N/A
Requisito OR.5	**Pautar el uso de dispositivos móviles.**
Objetivo	Garantizar la seguridad de la información de la organización en caso de utilizarse dispositivos móviles (al menos celulares, portables, tabletas) para uso laboral. Proteger la información de la organización, almacenada o accesible desde dispositivos móviles y evitar que éstos sean causa de distribución de software malicioso dentro de la organización o sean el origen de accesos no autorizados.
Alcance	Cualquier organización
Referencia ISO 27001	A.6.2.1
Guía de implementación	Se debe definir una política para el uso de dispositivos móviles que contemple, por ejemplo: gestión del inventario de los dispositivos móviles, medidas de protección física, pauta para uso y conexión fuera de las instalaciones de la organización, software permitido y versión, modo de conexión a los sistemas de información de la organización, métodos de control de acceso, uso de criptografía, medidas de protección contra software malicioso, bloqueo remoto de los dispositivos, respaldos, inventario de servicios y aplicaciones Web a los que puede accederse mediante los dispositivos móviles.
Administración Central	-
Instituciones de salud	Debe definirse una política de dispositivos móviles donde se indique específicamente si se podrá o no acceder a sistemas de historias clínicas desde dispositivos móviles y, en caso afirmativo, definir desde qué tipos de dispositivos se podrá acceder a estos sistemas. Asimismo, se deben establecer en la política las medidas de seguridad pertinentes para este tipo de dispositivos.

Guía de evidencia para auditoría	• Política de dispositivos móviles. • Procedimiento, manuales y/o instructivos para asegurar el adecuado uso de los dispositivos móviles. • Inventario de dispositivos móviles propiedad de la organización. • Inventario de dispositivos móviles personales pero que se conectan a algún servicio de la organización.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.16 Política de Dispositivos móviles
Requisito OR.6	Establecer controles para proteger la información a la que se accede de forma remota.
Objetivo	Garantizar la seguridad de la información cuando se accede de forma remota a los sistemas de información de la organización tanto por personal interno como externo.
Alcance	Cualquier organización
Referencia ISO 27001	A.6.2.2
Guía de implementación	Política y procedimiento de acceso remoto Se debe definir una política de acceso remoto donde se establezcan los requisitos necesarios de seguridad de las comunicaciones definiendo los motivos para el acceso remoto y el tipo de información a la que se accederá teniendo en cuenta su clasificación. Se debe contar con un procedimiento asociado a la política que indique al menos cómo es el procedimiento para la solicitud del acceso remoto. Mecanismos de autenticación y comunicaciones Se deben utilizar comunicaciones y mecanismos de autenticación seguros. Medidas de seguridad para el acceso remoto Se debe definir desde qué equipos se podrá acceder remotamente y qué medidas de seguridad tienen que tener dichos equipos, por ejemplo, protección contra software malicioso, últimos parches de actualización del sistema operativo, etc. Se debe evaluar la posibilidad de implementar el doble factor de autenticación para realizar conexiones remotas. Se debe contar con una lista blanca de todos los recursos disponibles accesibles de forma remota. Usuarios autorizados a acceder de forma remota Se debe determinar qué usuarios pueden acceder y autorizarlos; en qué momento, por cuanto tiempo y a qué recursos. Los usuarios deben ser nominados, evitando el uso de cuentas genéricas. Revisión periódica de los accesos remotos

	También se debe definir un procedimiento de revisión periódica de las cuentas de usuario con privilegios de acceso remoto y validar la necesidad de mantener dichos accesos. Protección de datos personales Se debe tener especial cuidado en aspectos como la comunicación y/o transferencia internacional de datos, teniendo en cuenta la normativa local de protección de datos (Ley 18.331).
Administración Central	-
Instituciones de salud	Controles relacionados a proveedores de equipamiento médico Se debe contar con controles tendientes a mitigar el riesgo relacionado al acceso remoto de los proveedores de equipamiento médico que requieren acceder por temas de mantenimiento. Protección de datos personales A nivel general, en el caso de los accesos remotos, se debe prestar especial cuidado en el intercambio transfronterizo de datos, particularmente la transmisión de información personal y de salud de los usuarios (historias clínicas) fuera de la jurisdicción nacional. Se debe tomar en cuenta lo dispuesto en la ley 18.331 “Protección de datos personales y acción de habeas data”, artículo 23 “Datos transferidos internacionalmente”, donde se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia. Asimismo, en el punto A del mismo artículo se menciona que es posible realizar la transferencia internacional de datos si el interesado ha dado su consentimiento inequívocamente a la transferencia prevista. La resolución 17/009 de la URCDP, indica cuáles son los países adecuados que básicamente son los que Europa reconoce como tales. En el caso de EEUU, al momento de la creación de la resolución regía el Puerto Seguro en materia de protección de datos, calidad que se otorga por empresas. Para cada transferencia a EEUU se debería revisar a qué empresa se transfieren los datos (actualmente Privacy Shield). Mecanismos de seguridad para el acceso remoto Se deberán utilizar mecanismos seguros para el acceso remoto, que garanticen la privacidad, confidencialidad e integridad de la información. El acceso remoto debería contar con mecanismos de activación y desactivación para realizar las tareas que sean necesarias con un plazo establecido. En aquellos casos para los que no sea posible contar con un plazo establecido, se deberá justificar el uso continuo de conexiones remotas.

Guía de evidencia para auditoría	• Política de acceso remoto. • Mecanismos de autenticación para la conexión remota documentados en la política. • Procedimiento de altas, bajas y modificaciones de acceso remoto. • Procedimiento de revisión de usuarios con acceso remoto. • Listado de servidores críticos que permiten acceso remoto. • Listado con la identificación de los usuarios habilitados para acceder remotamente a sistemas críticos.
Normativa asociada	Ley 18.331: Protección de datos personales, acción de habeas data Resolución 17/009 URDP.
Documentación de apoyo asociada	Anexo I - AI.24 Política de Acceso remoto

4.5 Gestión humana

Requisito GH.1	Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información.
Objetivo	Lograr que el personal comprenda sus responsabilidades de seguridad de la información y que apliquen la seguridad de la información de acuerdo a las políticas y los procedimientos establecidos.
Alcance	Cualquier organización
Referencia ISO 27001	A.7.1.2, A.7.2.3, A.7.3.1
Guía de implementación	Contratos En los contratos laborales con el personal, deben incluirse cláusulas relativas a la seguridad de la información que definan las responsabilidades. Procedimientos para la desvinculación Se recomienda contar con procedimientos formales a la hora de la desvinculación del personal, definiendo al menos la revocación de los derechos de acceso, tanto a nivel físico como lógico, además de las responsabilidades y acuerdos de no divulgación, estableciendo el tiempo que continuarán siendo válidos estos aspectos luego de la desvinculación. Proceso disciplinario Se recomienda contar con un proceso disciplinario, formalizado antes las autoridades, que contemple todos los aspectos legales internos cuando el personal incumpla con las políticas establecidas. También debe tenerse en cuenta para este procedimiento la normativa laboral a las que están sometidas las partes.
Administración Central	-
Instituciones de salud	Es recomendable que, al menos los roles y responsabilidades del personal que tenga acceso a datos personales y de salud, se encuentren debidamente documentados, indicando en cada caso el tipo de información al que puede acceder. Esto incluye también al personal que se desempeña de manera temporal en la institución de salud. Establecer los términos y condiciones de uso de cada sistema, como: HIS, LIS, RIS, entre otros.
Guía de evidencia para auditoría	• Listado de personal contratado en el período auditado. • Contratos firmados del personal que pertenezcan al período auditado. • Listado de personal desvinculado en el período auditado. • Evidencia de cumplimiento con las actividades definidas en los procedimientos de desvinculación de personal durante el período auditado, por ejemplo, planillas, formularios de solicitud de revocación de permisos, notas, cartas de

	desvinculación, correos donde se demuestre el cumplimiento con los procedimientos definidos, etc. • Acuerdos de no divulgación firmados del período auditado.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.23 Política de Finalización o cambio de relación funcional. Anexo II - AII.3 Compromiso de no divulgación – Personal.
Requisito GH.2	Concientizar y formar en materia de seguridad de la información a todo el personal.
Objetivo	Lograr conciencia de las responsabilidades y buenas prácticas vinculadas a la seguridad de la información de acuerdo a las políticas de seguridad de la información de la organización.
Alcance	Cualquier organización.
Referencia ISO 27001	A.7.2.1, A.7.2.2
Guía de implementación	<u>Participación de la Dirección y las Gerencias</u> La Dirección debe velar por proveer instrucción y orientación sobre seguridad de la información al personal para lograr una conciencia en relación con los roles y responsabilidades que corresponda. Tanto la Dirección como las Gerencias deberían tener una participación activa en las actividades de concientización. <u>Plan de concientización y formación</u> Se deben definir y ejecutar actividades o campañas de concientización y formación en materia de seguridad de la información de forma periódica. Es deseable que se elabore un plan o programa anual que abarque a todo el personal e identifique los distintos grupos estratégicos diferenciado el abordaje según sea conveniente. Este plan o programa debe estar alineado a la política de seguridad de la información definida y contar formalmente con los recursos necesarios para llevarlo a cabo. En el proceso de inducción se debe contemplar el abordaje inicial a la seguridad de la información. Se debe contar con planes de capacitación según roles y estos planes deben estar aprobados por la Dirección. El plan o programa de concientización para abordar la campaña, debe contemplar los actores críticos, objetivos, estrategia, táctica y audiencia y debe contar con indicadores para la medición del éxito de la campaña. <u>Materiales de concientización y formación</u> Los materiales de concientización deben ser completos, y pueden contener ejemplos de la vida diaria basada en los riesgos de ciberseguridad y las buenas prácticas. Además, estos materiales deben ser comprensibles y estar adaptados a la mayoría de los puestos de trabajo. <u>Formación de acuerdo al rol</u>

	El personal requiere una formación general y orientada al rol desempeñado. El personal de Seguridad de la Información y/o de Tecnología de la Información, así como el personal de Seguridad Física deben ser capacitados periódicamente. Se debe enfatizar la concientización y capacitación de los usuarios privilegiados. Difusión de políticas Las instancias de concientización y/o capacitación deben difundir las políticas y mecanismos de seguridad de la información que se impulsan en la organización, así como el uso adecuado de los activos a todo el personal y partes interesadas. Herramientas (ejemplos) Algunas herramientas que podrían utilizarse son: • Cursos de formación (internos y externos). • Canales de noticias. • Bases de conocimiento. • Herramientas de formación. • Redes sociales. • Correo electrónico. • Herramientas de colaboración. • Avisos de la industria y fabricantes. • Avisos CERTuy. • Charlas informativas.
Administración Central	-
Instituciones de salud	Es necesario que se cuente con esfuerzos específicos de capacitación y concientización en temas vinculados a seguridad de la información para el equipo de salud.
Guía de evidencia para auditoría	• Documentación que evidencie la ejecución del programa de concientización: realización de charlas, capacitaciones, divulgación, actividades de concientización, calificaciones obtenidas por los participantes, entre otros, que se hayan realizado en el período auditado. • Programa anual de concientización en seguridad de la información. • Material de sensibilización y capacitación. • Correos electrónicos, carteles, artículos. • Registros de capacitaciones ante la eventualidad de entrevistas aleatorias para evaluar el conocimiento sobre la política.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	N/A

4.6 Gestión de activos

Requisito GA.1	Identificar formalmente los activos de la organización junto con la definición de su responsable.
Objetivo	Garantizar la gestión de los activos asociados a la información y los sistemas e instalaciones para su procesamiento.
Alcance	Cualquier organización
Referencia ISO 27001	A.8.1.1, A.8.1.2
Guía de implementación	Inventario de activos Se debe identificar e inventariar los activos que contienen información y las instalaciones de su procesamiento, incluyendo todo activo que tenga asignada una IP. Asimismo, es necesario identificar el software de base y de aplicación. Es importante identificar la ubicación de los activos de información y, de ser posible, si se trata de un dispositivo móvil (celulares, notebooks, tablets, etc.) y/o si es personal o de la organización. Responsables de los activos Se debe identificar un responsable de gestión para cada activo mantenido en el inventario. Herramientas de apoyo Es recomendable la utilización de software de inventario que permita su clasificación y, cuando sea posible su uso, que se definan procesos que permitan la automatización del inventario. Dichos procesos (y/o procedimientos asociados) deben documentarse.
Administración Central	-
Instituciones de salud	Es recomendable identificar especialmente los activos de información que procesan y/o almacenan información de los usuarios (sistemas de historias clínicas, equipamiento médico, etc.). Es deseable que se identifique al responsable de la gestión del activo y al responsable técnico. Es necesario que todo aquel equipamiento que procese o almacene información de salud se ubique en el centro de datos. En aquellos casos que esto no sea posible, es necesario documentar la justificación y tomar las medidas de seguridad pertinentes y de similares características a las definidas en el centro de datos.
Guía de evidencia para auditoría	• Inventario de los activos de la organización. • Responsable de cada uno de los activos definidos en el inventario de activos.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo III - AIII.8 Guía para la rotulación de la información. Anexo IV - AIV.1 Guía metodológica - implantación SGSI. Anexo IV - AIV.2 Inventario de activos y Evaluación de riesgos.

Requisito GA.2	Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.
Objetivo	Proteger y garantizar la confidencialidad, integridad y disponibilidad de la información durante todo el ciclo de vida de los activos.
Alcance	Cualquier organización
Referencia ISO 27001	A.8.2.1, A.8.2.2
Guía de implementación	Se debe realizar un análisis y valoración de la información que posee con el fin de definir una clasificación apropiada, dependiendo de su valor, sus requisitos legales, la sensibilidad e importancia. Asimismo, se deben definir procedimientos para el etiquetado de los activos de acuerdo a la clasificación que se haya realizado. Se debe definir y revisar periódicamente las restricciones de acceso y la clasificación de los activos.
Administración Central	-
Instituciones de salud	<u>Protección de datos personales – datos sensibles</u> Según la ley 18.331 artículo 4, numeral E, los datos de salud son considerados datos sensibles. Se debe tomar en cuenta el artículo 19 de la mencionada ley que indica que: “Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los usuarios que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley”. <u>Confidencialidad de los CDA</u> Las instituciones deberían considerar la “Guía CDA Mínimo” para evaluar el nivel de confidencialidad de cada CDA (confidentialityCode) preestableciendo criterios de asignación. <u>Instituciones de salud pública</u> Las instituciones de salud pública deben clasificar la información de acuerdo a la ley 18.381. <u>Instituciones de salud privadas</u> En el ámbito privado, se recomienda clasificar la información de salud como confidencial. Asimismo, se debe clasificar el resto de la información de la institución, aunque no constituyan datos de salud, utilizando criterios de valoración y análisis de riesgos que la institución defina.
Guía de evidencia para auditoría	• Procedimiento de administración de activos. • Inventario de los activos de la organización. • Dueño de cada uno de los activos definidos en el inventario de activos. • Clasificación de cada uno de los activos definidos en el inventario de activos.

	• Procedimiento para el etiquetado de activos.
Normativa asociada	Ley 18.381: Derecho de acceso a la información pública. Ley 18.331: Protección de datos personales, acción de habeas data.
Documentación de apoyo asociada	Anexo I - AI.15 Política de Clasificación de la información. Anexo III - AIII.8 Guía para la rotulación de la información. Anexo IV - AIV.1 Guía metodológica - implantación SGSI. Anexo IV - AIV.2 Inventario de activos y Evaluación de riesgos Guía CDA Mínimo.
Requisito GA.3	Pautar el uso aceptable de los activos.
Objetivo	Garantizar que el personal, proveedores e interesados de la organización conozcan las reglas y tomen los recaudos necesarios para proteger los activos de la información de la organización.
Alcance	Cualquier organización
Referencia ISO 27001	A.8.1.3, A.11.2.6
Guía de implementación	Se debe definir una política donde se detalle el uso aceptable de los activos, el uso prohibido, responsabilidades, entre otros. Se recomienda pautar las reglas de uso de activos como: correo electrónico, aplicaciones, equipos, recursos de comunicación, uso de Internet, uso de redes sociales, etc y establecer los controles que realiza la organización y las responsabilidades de los usuarios. Es necesario formar e informar al personal en esta materia, para lograr la adecuada protección física y lógica de los activos.
Administración Central	-
Instituciones de salud	En el caso de las instituciones de salud, las pautas de uso aceptable de activos deben incluir al equipamiento médico.
Guía de evidencia para auditoría	• Política de uso aceptable de activos (genérica o específica para algún tipo de activo). • Evidencia de difusión de la política de uso aceptable de activos.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.3 Política de Uso aceptable de los activos. Anexo I - AI.27 Política de Uso institucional de redes sociales. Anexo I - AI.28 Política de Uso de Internet.
Requisito GA.4	Gestionar los medios de almacenamiento externos.
Objetivo	Proteger a la organización contra el acceso no autorizado a la información contenida en medios de almacenamientos externos, que son usados como repositorios o transporte de la información y así no permitir la divulgación, modificación u eliminación imprudencial o intencional de la información.
Alcance	Cualquier organización
Referencia ISO 27001	A.8.2.3, A.8.3.1, A.8.3.3

Guía de implementación	<u>Procedimiento para el manejo de medios de almacenamiento externos.</u> Se debe desarrollar un procedimiento para el manejo de medios de almacenamiento externo, tanto en las instalaciones de la organización como fuera de ella (Ver Requisito GA.3), que incluya las responsabilidades para su adecuado uso y protección. Este procedimiento debe difundirse entre el personal de la organización para su conocimiento y aplicación. <u>Inventario de medios de almacenamiento externos</u> Es necesario contar con un inventario de medios autorizados y definir procedimientos para su gestión que cubran como mínimo la solicitud, entrega, devolución y transporte de los medios de almacenamiento fuera de la organización. Se debe contar con procedimientos que indiquen cómo actuar ante casos de hurto, pérdida o daño del medio y difundirlos al personal. <u>Controles en medios de almacenamiento externos</u> Se deben establecer controles para bloquear el uso de dispositivos o medios de almacenamiento externos en las estaciones de trabajo, laptops y servidores a nivel físico de los puertos de los equipos y transferencias vía bluetooth que no sean necesarios, incorporando el principio de menor privilegio. <u>Medidas de protección</u> Si existen medios en reposo con información sensible, junto a otro tipo de información, el dispositivo debe ser considerado como contenedor de información sensible y, por tanto, deberá ser considerado con las mismas medidas que la organización haya establecido para ese tipo de información.
Administración Central	-
Instituciones de salud	Se debe contemplar la posibilidad de definir controles tendientes a mitigar el riesgo del almacenamiento de información sensible en diversos tipos equipamiento. En los casos, por ejemplo, de posibles envíos a reparación tanto de equipamiento médico como de equipamiento tradicional de oficina que contenga o pueda contener medios de almacenamiento, es necesario contar con medidas de control que impidan el acceso no autorizado a información sensible de salud. Se deben contar con una política para la gestión de la información que se encuentra almacenada dentro de los dispositivos biomédicos. Si existen medios en reposo con información de salud junto a otro tipo de información, el dispositivo debe ser considerado como contenedor de información de salud y, por tanto, deberá

	ser considerado con las mismas medidas que la institución haya establecido para ese tipo de información.
Guía de evidencia para auditoría	• Pautas para el manejo de medios de almacenamiento. • Listado de medios de almacenamiento externos utilizados por la organización. • Inventario de los activos de la organización con identificación de los medios de almacenamiento. • Procedimiento para la gestión de los medios de almacenamiento externos. • Evidencia de solicitudes, entrega o devolución de medios para el período auditado. • Evidencia de autorizaciones para transportar medios fuera de la organización. • Evidencias de medios de almacenamiento debidamente etiquetados. • Evidencia del mecanismo de encriptación de los medios.
Normativa asociada	Ley 18.331: Protección de datos personales, acción de habeas data.
Documentación de apoyo asociada	Anexo I - AI.4 Política de Traslado físico de la información. Anexo I - AI.14 Política de Intercambio de información.
Requisito GA.5	Establecer los mecanismos para destruir la información y medios de almacenamiento.
Objetivo	Garantizar la adecuada destrucción de la información y los medios de almacenamiento que la contienen, para proteger su confidencialidad.
Alcance	Cualquier organización
Referencia ISO 27001	A.8.3.1, A.8.3.2
Guía de implementación	Política y procedimiento Se debe definir una política y un procedimiento documentado para la destrucción de la información, que contemple los medios de almacenamiento para impedir la fuga de información contenida en ellos. Se deben establecer métodos para para la disposición final y borrado seguro de los medios de almacenamiento. El procedimiento debe contener los pasos para asegurar la eliminación lógica y física de la información (trituración, incineración, desmagnetización, borrado seguro, entre otros), según sea el caso y según lo determine cada organización. Eliminación y disposición Los métodos de eliminación elegidos deben asegurar que terceras partes no puedan acceder al medio luego de su disposición con el propósito de intentar recuperar información en forma no autorizada.

	Se deberán establecer en la medida que sea posible, puntos para la disposición de los medios de forma tal que estas actividades se realicen en forma coordinada.
Administración Central	-
Instituciones de salud	Resulta imprescindible contar con mecanismos de eliminación segura de la información de los medios de almacenamiento ya que no gestionar adecuadamente los procesos de destrucción de información podría generar una brecha de confidencialidad. Se debe contar con procedimientos formales que incluyan los pasos a seguir y deben considerarse también, no solo los equipos tradicionales de procesamiento de información, sino también el equipamiento médico que procese, registre y/o reporte información de las historias clínicas de los usuarios.
Guía de evidencia para auditoría	• Política de destrucción de medios de almacenamiento. • Procedimiento para la destrucción segura de medios de almacenamiento.
Normativa asociada	Ley 18.331: Protección de datos personales, acción de habeas data.
Documentación de apoyo asociada	Anexo I - AI.25 Política de destrucción de información Procedimientos – Procedimiento general para la destrucción de información Procedimientos - Bitácora de registro de destrucción de medios de almacenamiento

4.7 Control de acceso

Requisito CA.1	Gestionar el acceso lógico.
Objetivo	Gestionar y autorizar el acceso lógico a los activos de información (usuarios y usuarios privilegiados, aplicaciones, redes y servicios de red).
Alcance	Cualquier organización
Referencia ISO 27001	A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4 y A.9.2.6
Guía de implementación	<u>Controles de acceso lógico</u> Se debe contar con controles de acceso lógico basados al menos en usuarios y contraseñas. Se debe evitar el uso de cuentas genéricas (en especial, aquellas que requieran accesos privilegiados) que no sea posible identificar con un usuario particular. En caso de ser necesario contar con usuarios genéricos, por ejemplo para la ejecución de ciertas aplicaciones o servicios, su uso debe estar documentado y debidamente aprobado. <u>Política general de gestión de acceso lógico</u> Se debe definir una política de gestión de acceso lógico que aborde o al menos detalle los siguientes aspectos: • Autorización del acceso (a redes, a aplicaciones, etc.).

	• Identificación y autenticación (métodos de autenticación). • Cómo se gestionan las autorizaciones de acceso (definición de procedimientos), así como la gestión de los usuarios y contraseñas, la cual es recomendable que se realice en forma centralizada. • Acceso a dispositivos (definir el acceso a fotocopiadoras, escáneres, cámaras, grabadoras, equipos móviles, etc.). • Revisión periódica de los accesos lógicos. • Con relación al acceso a las redes (LAN, WiFi, etc.) y servicios de red, se deben indicar las redes y servicios a los cuales se permite acceder, los medios utilizados para el acceso (por ejemplo, VPN) y requisitos de autenticación, entre otros. <u>Procedimientos</u> Para lograr una adecuada gestión del acceso, se deben establecer procedimientos formales para las altas, bajas y modificaciones de usuarios y derechos de acceso, que incluyan el registro de todas las acciones. Estos procedimientos, detallan los responsables de asignar o revocar privilegios y el paso a paso de cómo se debe desarrollar la solicitud, con todas las autorizaciones necesarias. <u>Políticas complementarias de acceso lógico</u> Asimismo, las organizaciones deberían implementar (o configurar) políticas de acceso en todos los sistemas de información (sistemas operativos, aplicaciones, etc.). Por ejemplo, generar una política de gestión de contraseñas que se encuentre alineada a la política de gestión de acceso lógico y acceso a redes y servicios de red. Se recomienda establecer los requisitos mínimos que requieren las contraseñas, los nombres de usuario, duración mínima y máxima de las contraseñas, historial de contraseña, entre otros aspectos. Se debe definir una política específica para la gestión de usuarios privilegiados (redes, aplicaciones, bases de datos, etc.) y se deben definir revisiones periódicas. <u>Métodos de autenticación y verificación de identidad</u> En aquellos casos que se requiera una autenticación fuerte y verificación de identidad se podrá establecer la utilización de métodos alternativos (eID (cédula electrónica), token, factor de doble autenticación, etc.). <u>Definición de cuentas de usuario y control interno</u> Para la creación de los usuarios, es necesario contemplar la separación de funciones de acuerdo con los procesos de

	negocio para evitar posibles fraudes y accesos no autorizados. Se deben considerar principios como: menor privilegio (acceder solo a la información necesaria para cumplir con un legítimo propósito), necesidad de saber (solo se concede acceso a la información que se necesita saber), necesidad de utilizar (solo se da acceso a recursos de TI, información, activos de información, etc. que se requiere para llevar a cabo una tarea). Los usuarios con acceso privilegiado deberían contar con una identificación diferente a la que utilizan habitualmente en actividades del negocio donde no requieren de una cuenta privilegiada. Las cuentas de usuarios privilegiados deben ser revisadas periódicamente.
Administración Central	-
Instituciones de salud	<u>Acceso lógico a dispositivos médicos</u> Dentro de la política de gestión de acceso lógico se debe incluir también el acceso a los dispositivos médicos con los que cuente la institución. Debe evitarse el uso de usuarios genéricos en los equipos médicos. <u>Trazas o logs</u> Con relación a la generación de trazas o "logs", se debe tener en cuenta lo mencionado en el artículo 13 del decreto 242/017: "Todos los accesos a la historia clínica electrónica deben quedar debidamente registrados y disponibles. La información no podrá ser alterada o eliminada sin que quede registrada la modificación de que se trate. En caso de ser necesaria su corrección, se agregará el nuevo dato con la fecha, hora y firma electrónica del que hizo la corrección, sin suprimir lo corregido.". <u>Identificación y autenticación</u> Asimismo, en el artículo 18, se menciona: "Las instituciones con competencias legales en materia de salud, públicas y privadas, a los efectos de conectarse a la Red Salud y acceder a la Plataforma de Historia Clínica Electrónica Nacional deberán estar debidamente identificadas electrónicamente. Del mismo modo, deberán garantizar mediante mecanismos informáticos seguros la autenticación de las personas cuyo acceso autorizan, así como la privacidad y la integridad de la información clínica intercambiada, de forma que ésta no sea revelada ni manipulada por terceros.". <u>Gestión de accesos</u> Al momento del alta (y en principio, también al momento de la modificación) de usuarios, se debe determinar si dichos usuarios accederán o no a información de salud. Se debe definir específicamente la gestión de acceso del personal temporal (por ejemplo, residentes, pasantes, etc.) con acceso a información de salud de los usuarios y contar con

	procedimientos específicos para las bajas de usuarios de los sistemas, una vez que el personal abandona la institución. Para al acceso a las historias clínicas de los usuarios, es deseable que el acceso sea mediante doble factor de autenticación.
Guía de evidencia para auditoría	• Política de control de acceso lógico. • Política de gestión de usuarios y contraseñas. • Mecanismos de autenticación utilizados. • Esquema de seguridad de las aplicaciones críticas. • Listado de ingresos y egresos de funcionarios en el período auditado con detalle de su cargo y accesos otorgados o dados de baja (RRHH). • Formularios de solicitud de Alta/Baja de cuentas de usuario para acceso a equipos de red y comunicaciones, sistemas operativos, aplicativos, otros, para una muestra de funcionarios tomada del listado de ingresos y egresos obtenido de RRHH, para el período auditado. • Formularios de solicitud de modificaciones de privilegios de cuentas de usuario para acceso a equipos de comunicaciones, sistemas operativos, aplicativos y otros, dentro del período auditado. • Listados de altas y bajas de funcionarios a los equipos de comunicaciones, sistemas operativos y aplicativos (sistemas), dentro del periodo auditado.
Normativa asociada	Decreto 242/017
Documentación de apoyo asociada	Anexo I - AI.5 Política de control de acceso lógico. Anexo I - AI.6 Política de gestión de usuarios y contraseñas. Anexo I - AI.7 Política de gestión de usuarios de acceso privilegiado.
Requisito CA.2	**Revisar los privilegios de acceso lógico.**
Objetivo	Revisar y controlar periódicamente los derechos de acceso lógico a los activos de información (incluyendo los permisos de los usuarios privilegiados).
Alcance	Cualquier organización
Referencia ISO 27001	A.9.2.5
Guía de implementación	Se debe definir un procedimiento periódico para la revisión de los derechos de acceso lógico de todos los usuarios, incluidos los usuarios con acceso privilegiado, con asignación de responsables y documentación que evidencie la revisión realizada. En el caso de los usuarios privilegiados, se deben verificar periódicamente sus competencias para evaluar si dicho acceso está alineado con sus funciones en la organización. Se recomienda definir la periodicidad de las revisiones de acceso lógico. A la hora de la revisión, siempre se debe tener presente la necesidad de acceso y el otorgamiento del mínimo privilegio.
Administración Central	-
Instituciones de salud	Asegurar que los datos de salud de los usuarios son accedidos únicamente por personal autorizado y no por otros

	roles que no requieren conocimiento de este tipo de información.
Guía de evidencia para auditoría	• Política de control de acceso lógico. • Procedimiento de revisión de privilegio de acceso. • Listado de usuarios con acceso privilegiado. • Evidencia de la revisión de usuarios y usuarios privilegiados en el período auditado (en el caso de los usuarios privilegiados, se busca contar con evidencia de que la organización determina lo adecuado de su asignación).
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.5 Política de control de acceso lógico. Anexo I - AI.6 Política de gestión de usuarios y contraseñas. Anexo I - AI.7 Política de gestión de usuarios de acceso privilegiado. Procedimientos - Procedimiento general para la revisión de cuentas de usuario en Active Directory Procedimientos - Procedimiento general para la revisión de cuentas de usuario en Samba
Requisito CA.3	**Establecer controles criptográficos.**
Objetivo	Proteger la confidencialidad, autenticidad e integridad de la información digital.
Alcance	Cualquier organización
Referencia ISO 27001	A.10.1.1, A.10.1.2
Guía de implementación	La organización debe evaluar la oportunidad de utilizar controles criptográficos, por ejemplo, para proteger: la transmisión de información o su resguardo; acceso a las redes o sistemas, a los datos y servicios de información. Es recomendable: • Definir una política sobre el uso de controles criptográficos. • Determinar en qué casos se utilizarán dichos controles. • Definir responsables de implementar la política y los controles. • Determinar los responsables de la generación y gestión de las claves durante su ciclo de vida. Ejemplos de controles criptográficos: • Cifrado de discos duros o dispositivos móviles. • Cifrado de respaldos. • Cifrado de mensajes de correo electrónico (por ejemplo, usando claves PGP). • Comunicación por medios de canales seguros (por ejemplo, HTTPS, TLS). • Establecimiento de VPN para acceso remoto.
Administración Central	-
Instituciones de salud	A nivel de XDS, se puede utilizar el campo HASH, (*Hash* de los elementos del documento) para que, al recibir el documento se verifique la integridad.

	Todos los sistemas Web de las instituciones que intercambien o puedan intercambiar información de salud deberán utilizar protocolo HTTPS. Los respaldos de los sistemas que procesen información relacionada con la salud deben estar cifrados.
Guía de evidencia para auditoría	• Política y procedimientos para el uso de criptografía y control criptográfico. • Registro de revisión y actualización de estos protocolos. • Listado de sistemas desarrollados por la organización y aquellos que usan firma electrónica avanzada. • Listado de sistemas que soportan uso de dispositivos criptográficos. • Mecanismos de validación de firmas y de certificados electrónicos. • Soluciones utilizadas para la firma de transacciones.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.17 Política de Uso de controles criptográficos
Requisito CA.4	Establecer los controles para el uso de firma electrónica.
Objetivo	Lograr el cumplimiento con los lineamientos establecidos por la UCE y Agesic para el uso de firma electrónica avanzada.
Alcance	Cualquier organización.
Referencia ISO 27001	N/A
Guía de implementación	Cualquier sistema que necesite realizar una firma electrónica avanzada de persona jurídica o física debe cumplir con los siguientes requerimientos: Contexto de aplicación: todos los casos • El sistema debe contar con los mecanismos para realizar firmas electrónicas basadas en certificados electrónicos X509v3. • En caso de tratarse de firmas de usuarios el mecanismo de firma debe estar integrado a la transacción del usuario. • Se debe soportar la autenticación de usuario y firmas electrónicas de documentos utilizando la cédula digital. Evaluar la integración al servicio brindado por Agesic. Contexto de aplicación: Todos los casos de uso de firma electrónica. • Debe soportar el uso de dispositivos criptográficos para la firma electrónica (tokens, smart cards, HSM, etc.) • Deben utilizarse estándares y protocolos seguros que no estén considerados obsoletos o vulnerables. • Deben utilizarse los estándares de codificación de firmas propios de los tipos de documentos firmados (XADES, PDFSignature, etc.) • Cuando no exista un formato de firma para el documento, se debe utilizar CMS-CAdES.

	• Validación de certificados a través de OCSP (Online Certificate Status Protocol), CRL (Certificate Revocation List) o equivalente. • En particular con las transacciones críticas del sistema, se debe describir la solución diseñada para la firma de las transacciones. • Deberá contar con mecanismos de validación de firmas y de certificados electrónicos. • En caso de tratarse de firmas a nivel de servidor, se debe garantizar la adecuada protección de la clave privada. • Debe poder hacer uso de certificados electrónicos emitidos por cualquier prestador de servicio de certificación acreditados ante la UCE, siguiendo todos los lineamientos de dicha unidad. Contexto de aplicación: Cuando se necesita dejar constancia de fecha y hora de la firma, o si se necesita firma longeva. • Debe ser compatible con el RFC 3161 para la solicitud de sellos de tiempo tanto sobre HTTP como sobre TCP, y debe poder realizar firmas electrónicas incluyendo sellos de tiempo (con el formato del RFC 3161).
Administración Central	-
Instituciones de salud	Se debe utilizar firma electrónica avanzada de la Institución (persona jurídica) para los siguientes casos: a) Almacenar los documentos clínicos. b) Intercambiar documentos clínicos. c) Al recibir un CDA, validar la firma electrónica avanzada. Para cumplir con el punto a) los documentos clínicos deben almacenarse al menos, con firma electrónica común del médico y firma electrónica avanzada de la Institución. El simple logueo al sistema no alcanza como método de firma. La recomendación para el punto a) es que cada médico utilice la firma electrónica avanzada de persona física para firmar los documentos clínicos.
Guía de evidencia para auditoría	• Detalle técnico de la solución (aplicativo, módulo, etc.) que implementa firma electrónica avanzada.
Normativa asociada	Ley 18.600: Documento Electrónico y Firma Electrónica.
Documentación de apoyo asociada	Centro de recursos (https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/)

4.8 Seguridad física y del ambiente

Requisito SF.1	Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas.
Objetivo	Minimizar el riesgo de acceso no autorizado a los centros de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos) y proteger las instalaciones y equipos contra robos, daños o mal uso.
Alcance	Cualquier organización
Referencia ISO 27001	A.11.1.1, A.11.1.2, A.11.1.6, A.11.2.1
Guía de implementación	<u>Arquitectura y estructura de los centros de datos</u> Con relación a lo que sería la definición del perímetro de seguridad física, según se indica en el decreto 92/014, Arquitectura y Estructura: *"El sistema estructural del edificio debe ser de acero o de hormigón. Como mínimo, la estructura del edificio debe estar diseñada para soportar cargas de viento de acuerdo con los códigos de construcción aplicables para la ubicación en cuestión y de conformidad con las disposiciones de las estructuras designadas como instalaciones esenciales (por ejemplo, construcción de Clasificación III del Código Internacional de la Construcción).* *Debe prever protección contra los principales eventos físicos, intencionales o accidentales, naturales o artificiales, que podrían causar una falla en el mismo. Es requerido control de acceso físico, muros exteriores sin ventana, seguridad perimetral, CCTV y protección contra incendio".* <u>Aclaraciones sobre arquitectura y estructura</u> Los activos críticos de información deben estar alojados en centros de datos cuya estructura y la del edificio que la contiene sea suficientemente robusta para soportar los eventos climáticos habituales en Uruguay, como ser lluvias, tormentas eléctricas, vientos fuertes. Los materiales de dicha estructura no pueden ser inflamables ni livianos. El centro de datos no podrá estar localizado en un sitio expuesto a inundaciones. Tampoco puede estar ubicado en zona donde el acceso se pueda ver afectado por condiciones naturales o humanas. El sistema estructural del edificio debe ser de acero o de hormigón. Como mínimo, la estructura del edificio debe estar diseñada para soportar cargas de viento de acuerdo con los códigos de construcción aplicables para la ubicación en cuestión y de conformidad con las disposiciones de las estructuras designadas como instalaciones esenciales (por ejemplo, construcción de Clasificación III del Código Internacional de la Construcción).

	Los materiales de pisos, puertas y mamposterías tampoco podrán ser inflamables. Se recomienda además el uso de piso técnico elevado. Se debe contar con un mantenimiento adecuado de la estructura que impida la filtración de humedades hacia el interior de la misma. Las instalaciones eléctricas deben estar protegidas de forma tal que evite el contacto no deseado con humanos. Es deseable que la sala de energía esté separada de la sala de cómputo. Todo esto se complementa con el sistema de Video Vigilancia que debe existir y debe poder registrar toda actividad dentro del recinto. <u>Acceso físico</u> Con relación al control de acceso físico, en el decreto 92/014, Arquitectura y Estructura, se menciona aspectos de control de acceso: *"Es requerido control de acceso físico, muros exteriores sin ventana, seguridad perimetral, CCTV y protección contra incendio".* Se debe definir una política y procedimiento de control de acceso físico que incluya su gestión de autorizaciones. <u>Aclaraciones sobre acceso físico</u> Tal como se establece en las aclaraciones al decreto 92/014, se debe contar con sistema autónomo de control de acceso, con lectores de tarjetas magnéticas, identificación por Radiofrecuencia (RFID) o sistemas biométricos. Estos sistemas deben ser administrados remotamente y deben mantener información histórica de accesos al centro de datos. El acceso al Centro de Datos deberá estar asegurado y ser restringido. Para ello es requisito que los muros exteriores al recinto no tengan ventanas y se cuente con seguridad perimetral. Además, debe contar con sistemas cerrados de TV. Los activos del centro de datos deben estar protegidos con barreras físicas para prevenir daños, ya sea con o sin intención. Para esto se sugiere el uso de racks con puertas y cerraduras. <u>Política de control de acceso físico y procedimientos</u> Se debe contar con una política de control de acceso físico e implementar todos los procedimientos que se entiendan necesarios para su implementación. <u>Registro de accesos físicos</u> Se debe contar con un registro de visitantes, indicando entre otros datos, el motivo de la visita. Los registros de accesos físicos al centro de datos y áreas relacionadas o seguras deben revisarse en forma periódica y el procedimiento de revisión debe estar documentado.

Administración Central	Debe cumplir con lo establecido en el decreto 92/014.
Instituciones de salud	<u>Seguridad del equipamiento de los centros de datos y equipamiento médico</u> Es importante considerar especialmente la seguridad física del equipamiento, no solamente de los centros de datos y áreas relacionadas, sino también en las áreas de atención médica donde pueden existir equipos que, por razones de atención al usuario, puedan quedar expuestos y desatendidos. Por lo tanto, es necesario que se cuente con medidas de mitigación para estas situaciones como una política de pantalla y escritorios limpios que, entre otros temas, procure que cada vez que un equipo queda desatendido, por ejemplo, sea bloqueado. <u>Perímetros</u> Si bien es necesaria la definición de perímetros, seguramente existan casos en donde no sea del todo posible evitar que los usuarios ingresen a recintos donde existe equipamiento crítico conectado, por ejemplo, a la red de la Institución y con acceso o conexión a los sistemas de historias clínicas, dado que posiblemente ese equipamiento se encuentre relacionado al tratamiento de los usuarios o a las consultas médicas. <u>Política de control de acceso físico</u> En la política de control de acceso físico, se debe contemplar el control de acceso al equipamiento médico. <u>Dispositivos médicos móviles</u> Es recomendable contar con un recinto, con control de acceso, donde se pueda almacenar los dispositivos médicos móviles (por ejemplo, bombas de infusión inalámbricas) cuando no estén siendo utilizados.
Guía de evidencia para auditoría	• Política de control de acceso físico. • Procedimientos de control de acceso físico incluyendo la gestión de autorizaciones. • Listado de áreas seguras y personas autorizadas a acceder. • Registros de accesos físicos en áreas seguras para el período auditado.
Normativa asociada	Decreto 92/014
Documentación de apoyo asociada	Anexo I - AI. 8 Política de control de acceso físico a áreas seguras. Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.
Requisito SF.2	**Implementar controles ambientales en los centros de datos y áreas relacionadas.**
Objetivo	Garantizar la continuidad de las operaciones y reducir los efectos causados por desastres humanos o naturales a través de la implementación de controles ambientales en los centros

	de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos).
Alcance	Cualquier organización
Referencia ISO 27001	A.11.1.4, A.11.2.1, A.11.2.3
Guía de implementación	<u>Política de seguridad del equipamiento</u> Debe definirse una política de seguridad del equipamiento. Dicha política puede contener, entre otros, los siguientes puntos: medidas de protección y ubicación del equipamiento crítico de la organización, controles para la protección de amenazas físicas y/o ambientales, mecanismos de monitoreo de condiciones ambientales, medidas para el manejo del equipamiento fuera de las instalaciones de la organización, etc. <u>Controles ambientales</u> Se puede tomar como base el apartado del decreto 92/014: "Arquitectura y Estructura": *"Debe prever protección contra los principales eventos físicos, intencionales o accidentales, naturales o artificiales, que podrían causar una falla en el mismo. Es requerido control de acceso físico, muros exteriores sin ventana, seguridad perimetral, CCTV y protección contra incendio."* <u>Aclaraciones sobre los controles ambientales</u> Se debe contar con sistema de detección y extinción de incendios. Éste debe contar con mantenimiento periódico que asegure su correcto funcionamiento. En caso de incendio, ya sea dentro o fuera del centro de datos, el fuego no debe traspasar la barrera física del centro de datos por el mayor tiempo posible. El sistema de climatización debe implementarse con varias unidades de aire acondicionado cuya capacidad de refrigeración combinada mantenga constantes la temperatura y la humedad relativa a las condiciones de diseño del espacio crítico, incluso en caso de fallo de al menos una unidad de aire acondicionado. Los activos de centro de datos están diseñados para funcionar en un ambiente controlado de temperatura y humedad. Dadas las condiciones climáticas de Uruguay y sumado a que el equipamiento disipa importantes cantidades de calor, es necesario contar con sistemas de aire acondicionado para mantener la temperatura controlada en las condiciones de diseño. Del mismo modo, la humedad del ambiente también deberá mantenerse dentro de valores controlados.
Administración Central	Debe cumplir con lo establecido en el decreto 92/014.
Instituciones de salud	El control ambiental de los recintos donde se cuenta con equipamiento informático y/o equipamiento médico debe planificarse considerando el ambiente específico del área

	salud. Existe equipamiento que debe ser protegido, por ejemplo, contra emisiones electromagnéticas. A su vez todo equipo que se utilice para procesar o almacenar información debe protegerse del equipamiento médico que pueda afectarlo y provocar, por ejemplo, fallos o indisponibilidad de los sistemas.
Guía de evidencia para auditoría	• Habilitación de bomberos. • Contratos con proveedores (alarmas, aire acondicionado, etc.). • Protección ambiental (alarma, extintores, sistemas de extinción, aire acondicionado, etc.). • Ubicación de la sala de cómputo y la sala de energía.
Normativa asociada	Decreto 92/014
Documentación de apoyo asociada	Anexo I - AI.9 Política de seguridad del equipamiento. Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.
Requisito SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.
Objetivo	Lograr una adecuada administración de los componentes críticos alojados en sitios o centros de datos.
Alcance	Cualquier organización
Referencia ISO 27001	A.11.2.2, A.11.2.4, A.12.4.1, 12.4.2, 12.4.3, 12.4.4
Guía de implementación	Procedimiento de monitoreo Se debe definir un procedimiento documentado de monitoreo que incluya el uso de herramientas automatizadas para realizar estas tareas, en los casos que aplique. Sistema de gestión y monitoreo Para la implementación de este requisito, se puede tomar como base el decreto 92/014. Este establece la recomendación de contar con un sistema de gestión y monitoreo centralizado que pueda alertar fallas en componentes críticos del centro de datos. Aclaraciones sobre el sistema de gestión y monitoreo Para administrar correctamente un centro de datos y sitio de contingencia, es necesario que se realice un monitoreo permanente de todas las variables ambientales, del estado de salud de los activos e incluso de los servicios informáticos que se brindan desde el centro de datos. Existen varios tipos de monitoreo. Una posible clasificación es: informativo, preventivo y reactivo. El monitoreo preventivo permite analizar con base en el histórico, la situación actual el comportamiento futuro de la infraestructura y sistemas de información. El mantenimiento histórico de los valores monitoreados no solo permite pronosticar tendencias, sino que puede aportar información valiosa en análisis forenses de incidentes o eventos no esperados.

	El monitoreo reactivo es el encargado de “disparar” alarmas en caso de fallas o umbrales definidos para prevenir eventos no deseados. Este tipo de monitoreo deberá realizarse y ser atendido en una modalidad 7x24 para los eventos críticos. Estas alarmas deberán clasificarse según su severidad desde informativas a críticas, siendo estas últimas las que deben atenderse de forma inmediata. <u>Herramientas de monitoreo</u> Las herramientas más comunes para consolidar monitoreo implementan protocolos como SNMP, ICMP, HTTP, consulta de apertura de puertos TCP y permiten realizar scripts para obtener valores a graficar. Las mismas herramientas permiten definir umbrales y enviar alarmas por mail, en tiempo real en un cuadro de mando. Es deseable contar con herramientas para cruzamiento de información de diversas fuentes que permitan emitir alertas preventivas. Se debe establecer una estrategia de recolección de la información, evitando un único punto de falla. <u>Monitoreo alternativo</u> Se debe contar con alternativas de monitoreo (al menos manual) ante fallas del mecanismo principal. <u>Plan de mantenimiento</u> Se debe definir un plan que permita establecer las acciones preventivas y correctivas de todo el equipamiento que se encuentre dentro y fuera de los centros de datos, a fin de mantener la adecuada disponibilidad de los componentes críticos, apoyado en los procesos de monitoreo para detectar alertar ante fallas, con el objetivo de prevenir daños y realizar el mantenimiento en los tiempos recomendados por los proveedores.
Administración Central	Debe cumplir con lo establecido en el decreto 92/014.
Instituciones de salud	Todo equipamiento clínico que almacene o procese información de salud de los usuarios debe ser monitoreado con el fin de, por ejemplo, verificar que se encuentre funcionando de acuerdo a lo esperado según su función en el proceso asistencial.
Guía de evidencia para auditoría	• Herramientas utilizadas para el monitoreo. • Procedimiento de monitoreo. • Plan de mantenimiento. • Reportes de fallas y alertas dentro del período auditado. • Evidencia de la revisión de fallas y alertas dentro del período auditado. • Registro del mantenimiento histórico de los valores monitoreados dentro del período auditado. • Bitácora de acceso de personal interno o externo que realice las actividades o labores de mantenimiento al equipamiento en general.

	• Documentación de los controles de cambio para el mantenimiento de los componentes críticos.
Normativa asociada	Decreto 92/014 (Anexo III).
Documentación de apoyo asociada	Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.

4.9 Seguridad de las operaciones

Requisito SO.1	Gestionar las vulnerabilidades técnicas.
Objetivo	Prevenir y mitigar el riesgo de explotación de vulnerabilidades técnicas en los sistemas.
Alcance	Cualquier organización.
Referencia ISO 27001	A.12.6.1
Guía de implementación	Inventario de activos En el inventario de activos de la organización debe incluir información como: proveedor del software instalado, versión, fecha de instalación, estatus (producción, test, desarrollo), entre otros. Plan o Pautas para la gestión de vulnerabilidades y parches Se deben definir un plan o pautas para la gestión de vulnerabilidades y parches que aborden, entre otros, los siguientes puntos: • Roles y responsabilidades para la gestión de vulnerabilidades y parches. • Procedimiento para la identificación de las vulnerabilidades técnicas través de terceras partes (foros, CERTuy, etc.) y aquellas detectadas en forma interna a la organización. • Se definen otras fuentes de identificación de vulnerabilidades a través de escaneos de infraestructura y aplicaciones. • Evaluación de riesgos, clasificación y priorización de las vulnerabilidades técnicas detectadas. • Cronograma para llevar adelante las acciones correctivas de las vulnerabilidades técnicas. • Evaluación de los parches de seguridad que sean necesarios aplicar a la instalación (análisis de riesgo de la vulnerabilidad vs análisis de riesgo de la instalación del parche). • Ambiente para probar los parches, previo a su puesta en producción. Los parches y las acciones correctivas de las vulnerabilidades técnicas detectadas deben ser llevadas a cabo y puestos en producción en función del procedimiento de gestión de cambios (considerando si corresponde el procedimiento de gestión de cambios de emergencia) y el proceso de gestión de incidentes

	• Controles a implementar en caso de que no se cuente con ningún parche para aplicar frente a una vulnerabilidad. • Deben definirse controles compensatorios para aquellos activos que por su tecnología no puedan ser actualizados con los últimos parches de seguridad.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Inventario de activos. • Pautas para la gestión de vulnerabilidades y parches. • Procedimiento para la gestión de vulnerabilidades y parches. • Registro de vulnerabilidades y parches, y detalle de su tratamiento internamente en la organización en el período auditado. • Procedimiento de gestión de cambios. • Procedimiento de gestión de cambios de emergencia. • Procedimiento de gestión de incidentes. • En función de los sistemas operativos utilizados, obtener una lista de las actualizaciones críticas para cada uno y comparar contra las actualizaciones realmente realizadas. • Evidencia del análisis realizado por la organización acerca de los cambios previo a instalar un parche (para una muestra de parches en el período auditado).
Normativa asociada	N/A
Documentación de apoyo asociada	N/A
Requisito SO.2	**Gestionar formalmente los cambios.**
Objetivo	Asegurar que los cambios no comprometan la seguridad. Lograr un adecuado control y seguimiento de los pedidos de cambio de los sistemas y configuraciones de componentes de la infraestructura, asegurar que los cambios están justificados y autorizados, que se llevan a cabo sin perjuicio de la calidad del servicio y se encuentran registrados, clasificados, documentados y probados de manera adecuada.
Alcance	Cualquier organización
Referencia ISO 27001	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
Guía de implementación	<u>Alcance de la gestión de los cambios</u> Si bien la gestión de los cambios debe existir y ser formal a nivel de todas las áreas la organización, se debe establecer al menos, un control formal de los cambios en el ámbito tecnológico. Aplica a todo tipo de cambios tecnológicos, como cambios en configuraciones de servidores, sistemas operativos, firewalls y aplicaciones, entre otros. <u>Política de gestión de cambios</u> La política de gestión de cambios debería abordar temas tales como: • Solicitud.

	• Registro. • Autorización. • Evaluación de riesgos e impacto. • Priorización. • Ejecución, prueba y aprobación. • Gestión de configuración. • Prever la posibilidad de volver atrás para la recuperación a un estado estable conocido anterior en caso de imprevistos o errores. • Control de versionado y línea base. • Cambios de emergencia, es decir aquellos que por su urgencia no pueden realizarse según lo establecido en el procedimiento de gestión de cambios tradicional. • Herramientas disponibles en la organización para dar soporte a la gestión de los cambios. <u>Procedimiento de gestión de cambios</u> Para cada tipo de cambio, se recomienda contar con un procedimiento que acompañe la política, donde se detallen los responsables, las actividades y las herramientas de gestión que apoyan el procedimiento si existieren. Independientemente de la existencia o no de herramientas de apoyo para la gestión, los cambios deben ser siempre registrados.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Política de gestión de cambios. • Procedimiento para la gestión de cambios. • Procedimiento para cambios de emergencia. • Listado (muestra) de cambios en el período auditado. • Evidencia para una muestra de cambios dentro del período auditado, para verificar que se ha cumplido con los procedimientos definidos de gestión de cambios (análisis de riesgos, aprobación, etc.). • Listado (muestra) de cambios de emergencia en el período auditado. • Evidencia de la realización de las actividades descriptas en los procedimientos: análisis de riesgos, autorización, aprobación, registro, etc. • Pautas de desarrollo seguro. • Metodología de desarrollo incluyendo aspectos de seguridad.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.22 Política de Gestión de cambios
Requisito SO.3	Gestionar la capacidad de los servicios y recursos que se encuentran operativos.
Objetivo	Asegurar que la capacidad de servicios de TI y la infraestructura de TI, sean capaces de cumplir con los objetivos

	acordados de capacidad y desempeño de manera puntual y efectiva en términos económicos.
Alcance	Cualquier organización
Referencia ISO 27001	A.12.1.3
Guía de implementación	<u>Alcance de la gestión de la capacidad</u> Una reducción en la calidad de los servicios críticos o interrupciones de éstos debido a que la infraestructura disponible no sea suficiente para soportar la demanda puede tener consecuencias en operaciones de la organización. Si bien la gestión de la capacidad debe ser lo más amplia posible, se entiende que al menos se debe enfocar a la gestión de la capacidad de los servicios críticos. <u>Identificación de los requisitos de capacidad</u> Para lograr esto, es necesario en primer lugar, lograr la identificación de los activos (servicios, sistemas y recursos) críticos para la organización. Posteriormente, se debe identificar los requisitos de capacidad para esos activos críticos. Se debería poder realizar mediciones objetivas para detectar problemas de capacidad. <u>Plan de gestión de la capacidad</u> Se debe elaborar un plan de gestión de la capacidad. Para ello es necesario conocer o definir al menos: • Alcance del plan de capacidad. • Responsables y roles. • Las operaciones de negocio actuales (al menos las críticas) y los requerimientos asociados a ellas. • Los planes de negocio futuros. • Acuerdos de nivel de servicio. • Actividades de supervisión de los recursos más relevantes (aquellos que son más costosos o cuya adquisición lleva mucho tiempo). • Estimaciones sobre la cantidad de recursos que se requerirán a futuro en los próximos años (ejemplo, 1,2 o 3 años). • Obtener información que determine las tendencias o los cambios en la utilización de los recursos. • Períodos pico o bajas (peak times – down times). • Estudios de aumento de capacidad o disminución de la demanda (estrategia a seguir), por ejemplo: lograr espacio en disco eliminando datos que ya no se utilizan, desinstalar aplicaciones que no se utilizan, así como sus bases de datos, optimización de procesos por lotes, optimización de consultas en las bases de datos, estudiar el uso del ancho de banda de los servicios críticos para evaluar si se puede negar o restringir el uso del mismo, entre otros.

	• Recomendaciones necesarias para el o los períodos futuros. • Revisiones del plan a intervalos regulares.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Plan de capacidad. • Registros que demuestren que se han realizado mediciones de los recursos críticos (hardware, software, etc.) en el período auditado. • Actividades realizadas para proporcionar o mejorar la capacidad en el período auditado, de acuerdo al plan de capacidad.
Normativa asociada	N/A
Documentación de apoyo asociada	N/A
Requisito SO.4	**Definir entornos separados para desarrollo, pruebas y producción.**
Objetivo	Reducir los riesgos de accesos no autorizados o realización de cambios no autorizados en producción, evitar modificaciones no deseadas de archivos o sistemas, evitar fallas de los sistemas.
Alcance	Cualquier organización.
Referencia ISO 27001	A.12.1.4, A.14.3.1
Guía de implementación	Política de separación de ambientes Se debe contar con una política que determine la separación de ambientes para desarrollo, pruebas, producción y procedimientos afines. Los tres ambientes deben estar claramente identificados para reducir posibilidad de errores y deben existir responsables para su gestión, quienes deben participar desde el inicio en los proyectos. Segregación de ambientes Se recomienda que los ambientes de desarrollo y pruebas se encuentren segregados del ambiente de producción. Procedimiento para el pasaje a producción Se recomienda elaborar un procedimiento para el pasaje a producción que incluya, al menos, solicitud, autorización, responsables, verificación de operatividad y plan de marcha atrás. Procedimiento de pruebas Es necesario, además, definir un procedimiento de pruebas (testing) de sistemas y los pasos para la obtención de datos para pruebas evitando usar información sensible, confidencial, reservada o secreta. En caso de ser necesario el uso de estos datos para la realización de las pruebas, el contenido debería eliminarse o modificarse.

	En caso de requerir la copia de información de producción al ambiente de prueba, se debe contar con procedimientos de autorización y también deben tomarse los recaudos necesarios respecto a la clasificación de la información contenida (eliminar o modificar).
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Política de separación de entornos. • Procedimiento para el pasaje a producción. • Procedimiento o metodología de pruebas. • Documentación que detalle los diferentes ambientes existentes. • Listado de sistemas en desarrollo y producción y ambientes definidos. • Lista de cambios realizados en el período auditado. • Registro de solicitudes de cambio, análisis de riesgos, aprobaciones, rechazos de cambios y de los pasajes entre ambientes. • Ambientes de desarrollo, producción y pruebas para los sistemas seleccionados.
Normativa asociada	Ley 18.331: Protección de datos personales, acción de habeas data.
Documentación de apoyo asociada	Anexo I - AI.12 Política de Separación de entornos.
Requisito SO.5	**Controlar software malicioso.**
Objetivo	Asegurar que la información y los sistemas informáticos que la procesan se encuentren protegidos contra software malicioso (por ejemplo: virus, gusanos, troyanos, spyware, adware intrusivo, crimeware, entre otros).
Alcance	Cualquier organización.
Referencia ISO 27001	A.12.2.1
Guía de implementación	Política de control contra software malicioso Se debe contar con una política de protección contra software malicioso y procedimientos asociados que contemplen aspectos como: • Mecanismos y/o procedimientos para la detección de uso de software no autorizado o malicioso. • Mantener una lista de software autorizado (lista blanca). • Mantener una lista de sitios Web maliciosos y/o no autorizados (lista negra). • Protección antivirus centralizada y su responsable para la gestión. • Capacitar al personal afectado en la operación y uso de la solución antivirus, así como cualquier otro mecanismo utilizado para la detección de software malicioso. • Reducir las vulnerabilidades que podrían ser explotadas por software malicioso mediante, por ejemplo, la gestión técnica de vulnerabilidades.

	• Procedimientos para obtener información en forma regular (suscripción a listas de correo, comprobación de los sitios Web especializados que brindan información sobre nuevo software malicioso). Herramientas de monitoreo Se debe contar con herramientas automatizadas (antivirus, antispyware, firewalls personales, IPS, etc.), de preferencia centralizadas, para monitorear continuamente estaciones de trabajo, servidores y dispositivos móviles.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Política de Seguridad de la Información. • Política de protección contra software malicioso y otros archivos provenientes de redes externas u otros medios y medidas preventivas que deberán tomarse. • Procedimiento para el control y detección de software no autorizado o malicioso. • Lista de aplicaciones permitidas. • Lista de aplicaciones no permitidas. • Sitios Web no autorizados o reglas que los filtran. • Muestra de equipos para determinar que cuentan con el antivirus actualizado. • Muestra de equipos para determinar que cuentan con las últimas actualizaciones de seguridad instaladas. • Muestra de equipos para determinar que tienen instalado únicamente el software permitido. • Política y procedimiento de gestión de incidentes. • Muestra de incidentes y su gestión para una muestra seleccionada por el auditor dentro del período auditado. • Filtros aplicados en correo y Gateway.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.11 Política de Protección contra software malicioso
Requisito SO.6	**Respaldar la información y realizar pruebas de restauración periódicas.**
Objetivo	Preservar la información de la organización o en poder de ésta y poder restaurarla en tiempo y forma en caso de necesidad.
Alcance	Cualquier organización
Referencia ISO 27001	A.12.3.1
Guía de implementación	Política de respaldos Se debe definir una política de respaldos donde se detalle claramente los requisitos que posee la organización con relación a las copias de la información y sistemas. Plan de respaldos Conjuntamente, debe elaborarse un plan de respaldos (con procedimientos asociados) que contemple al menos: frecuencia, grado (completo, diferencial, incremental), período

	de retención (teniendo en cuenta la normativa que pueda existir), almacenamiento de los medios (dentro y fuera de la organización), pruebas periódicas sobre los respaldos, cifrado de los respaldos (si la organización así lo define ante requerimientos de confidencialidad), herramienta utilizada para los respaldos. Control de acceso a los respaldos Se establecen al menos, mecanismos de control de acceso lógicos y físicos a los respaldos. Se deben realizar revisiones de los respaldos a intervalos regulares y dicha periodicidad debe verse reflejada en la política. Pruebas periódicas a los respaldos Los respaldos deben ser probados regularmente y los procedimientos de pruebas y sus resultados deben documentarse. Registros Asimismo, es necesario definir registros o bitácoras para registrar la realización de los respaldos y sus actividades de supervisión, así como las fallas o problemas detectados y sus acciones correctivas. Revisiones periódicas Ante cambios en requerimientos del negocio, se debe revisar la política, plan y procedimientos y actualizarlos si corresponde.
Administración Central	Al momento de planificar los respaldos, se debe cumplir con lo indicado en el decreto N° 92/014, artículo 3: “Los sistemas informáticos (art. 3° del Decreto N° 451/009 de 28 de setiembre de 2009) de la Administración Central deberán estar alojados en centros de datos seguros situados en territorio nacional, exceptuándose aquellos que no constituyan un riesgo para el organismo, de acuerdo con los "Lineamientos para la implementación y uso de centros de datos seguros", que se anexa y forma parte del presente Decreto (Anexo III).”
Instituciones de salud	Al momento de planificar los respaldos se debe contemplar lo indicado en la ley 18.331 “Protección de datos personales y acción de habeas data”, artículo 23 “Datos transferidos internacionalmente” donde se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia. Asimismo, en el punto A del mismo artículo se menciona que es posible realizar la transferencia internacional de datos si el interesado ha dado su consentimiento inequívocamente a la transferencia prevista. La resolución 17/009 de la URCDP, indica cuales son los países adecuados que básicamente son los que Europa

	reconoce como adecuados. En el caso de EEUU regía al momento de la creación de la resolución el Puerto Seguro en materia de protección de datos, calidad que se otorga por empresas. Para cada transferencia a EEUU se debería revisar a qué empresa se transfieren los datos (actualmente Privacy Shield). La URCDP en dictamen 08/2014 de fecha 23/7/2014 dictaminó que el almacenamiento en una nube que no se encuentra en territorio nacional, se trata de una transferencia internacional de datos.
Guía de evidencia para auditoría	• Política de respaldos. • Plan de respaldos. • Registro (muestra) de los respaldos realizados para el período auditado. • Bitácora de la herramienta utilizada para los respaldos con detalle de respaldos realizados. • Listado de pruebas de restauración (muestra) realizadas en el período auditado. • Prueba de restauración de una muestra de archivos o carpetas seleccionadas. • Registros donde se documente las actividades de supervisión de los respaldos e inconvenientes o fallas encontradas.
Normativa asociada	Ley 18.331: Protección de datos personales y acción de habeas data. URCDP - Resolución 17/009 URCDP - Dictamen 08/2014 de fecha 23/7/2014 Otras que puedan establecer periodos de retención y otros requisitos asociados.
Documentación de apoyo asociada	Anexo I - AI.10 Política de Respaldo de información
Requisito SO.7	Registrar y monitorear los eventos de los sistemas.
Objetivo	Conocer los eventos relevantes que se suceden en una aplicación o sistema, por ejemplo, inicios de sesión, fallas en los sistemas, eventos de seguridad, etc. Asegurar la protección de los registros de eventos contra modificaciones y/o accesos no autorizados y asegurar los registros de auditoría.
Alcance	Cualquier organización
Referencia ISO 27001	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
Guía de implementación	Política de auditoría y registro de eventos y procedimiento asociado Se debe definir una política de auditoría y registro de eventos que incorpore procedimientos para la gestión y protección de los registros de eventos. Se debería contar con un procedimiento asociado a la política donde se identifiquen los eventos de los activos a monitorear y se establezcan umbrales tolerables para estos (por ejemplo, tiempo de espera para una

	aplicación Web, etc.). Se deben identificar las herramientas que se utilizarán para realizar el monitoreo. La política de auditoría y registro de eventos debe incluir lineamientos para registrar las actividades realizadas por los administradores y operadores del sistema y el control de éstas, por ejemplo, mediante la utilización de un sistema de detección de intrusos que se encuentre administrado fuera del control de administradores de sistemas y redes. Asimismo, dicho procedimiento debe contar con los pasos a seguir para la realización de actividades, responsabilidades, etc. <u>Registro de eventos de sistemas y usuarios</u> Es recomendable habilitar el registro de eventos a nivel de sistema operativo con el enfoque que la organización determine en función de sus requisitos de seguridad. A nivel de usuario, se deberían registrar los intentos de inicios de sesión fallidos, acceso y uso de Internet, y eventos relevantes que sucedan en sistemas o aplicaciones críticas. Asimismo, se debería evaluar la viabilidad de utilización de herramientas de apoyo para la gestión de los eventos y alarmas. Los registros de eventos o la auditoría de los sistemas informáticos deben estar habilitados en función de los requisitos de seguridad y deberían centralizarse para facilitar su revisión y estar protegidos contra accesos no autorizados. Se debería establecer y gestionar una línea base de operaciones de red y flujos de datos esperados para los usuarios y sistemas. Los registros de eventos deben ser respaldados fuera de línea en forma periódica. <u>Revisiones periódicas de los registros</u> Se debe establecer un procedimiento de revisión periódica de los registros generados y definir los responsables de la realización y periodicidad de las revisiones. <u>Sincronización de relojes</u> Los relojes de todos los sistemas de procesamiento de información se pueden sincronizar con una fuente de tiempo exacta (por ejemplo, servidores NTP), esto permite, por ejemplo, el seguimiento y la reconstrucción de las actividades.
Administración Central	-
Instituciones de salud	En relación con la generación de trazas o “logs”, se debe tener en cuenta lo mencionado en el artículo 13 del decreto 242/017: “Todos los accesos a la historia clínica electrónica deben quedar debidamente registrados y disponibles. La información no podrá ser alterada o eliminada sin que quede registrada la modificación de que se trate. En caso de ser necesaria su

	corrección, se agregará el nuevo dato con la fecha, hora y firma electrónica del que hizo la corrección, sin suprimir lo corregido.”
Guía de evidencia para auditoría	• Política de auditoria y registro de eventos. • Configuración del registro de eventos. • Herramientas utilizadas para el monitoreo de los eventos, excepciones y fallas utilizadas y su configuración. • Procedimiento de revisión periódica de los registros generados. • Procedimiento de detección y monitoreo. • Muestra de las revisiones periódicas realizadas durante el período auditado. • Muestra de las revisiones realizadas sobre las actividades de los administradores de sistemas y redes en el período auditado.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.13 Política de registro y auditoría de eventos
Requisito SO.8	Gestionar la instalación de software.
Objetivo	Garantizar la integridad y seguridad de los sistemas.
Alcance	Cualquier organización.
Referencia ISO 27001	A.12.5.1, A.12.6.2
Guía de implementación	<u>Procedimientos de instalación de software</u> Se recomienda definir procedimientos sobre la instalación de software y difundirlo a los usuarios y/o todo aquel interesado que se considere pertinente. Dentro de los temas a abordar en los procedimientos se encuentran los siguientes: • Instalación de software en equipamiento de usuario final. • Definición de los responsables de realizar las actividades de instalación de software en producción. • Pruebas previas al pasaje a producción de aplicaciones o sistemas operativos. • Referencia a procedimientos de vuelta atrás. • Registro de las actualizaciones en producción. • Software permitido y restricciones: - Tipo de software que pueden instalar los usuarios. - Software base. - Software prohibido. - Software que requiere autorizaciones especiales. • Revisiones periódicas sobre el software instalado en producción y en equipos de usuario. <u>Gestión de licencias de software</u> Es recomendable contar con un procedimiento para la administración de las licencias de software (solicitud/autorización, adquisición, instalación) y realizar

	control y revisión de las licencias instaladas (incluyendo periodicidad y responsables). Instalación de software por parte de los usuarios Es recomendable que dentro de las políticas de seguridad de la organización se contemple qué privilegios se les asignará a los diferentes usuarios con relación a la posibilidad de instalar software en sus equipos.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Procedimiento de instalación de software. • Procedimiento para la administración de las licencias de software. • Resultados de auditorías o revisiones internas sobre software instalado. • Listado de software instalado en los equipos dentro del período auditado. • Listado de software base permitido. • Listado de software especial y usuarios autorizados a su instalación. • Requerimientos a nivel legal y normativo para la instalación y uso de las licencias de software.
Normativa asociada	N/A
Documentación de apoyo asociada	N/A

4.10 Seguridad de las comunicaciones

Requisito SC.1	Los portales Web institucionales de los organismos de la Administración Central y sus dependencias deben identificarse con la extensión “gub.uy” y “mil.uy”, según corresponda.
Objetivo	Estandarizar la identificación de los portales Web institucionales de la Administración Central.
Alcance	Administración Central.
Referencia ISO 27001	N/A
Guía de implementación	Todos los servicios vinculados con Internet de los organismos de la Administración Central deben utilizar los nombres de dominio gub.uy o mil.uy, este último para el Ministerio de Defensa. Es decir que no podrán existir servicios vinculados a Internet de organismos de la Administración Central con un nombre de dominio diferente a gub.uy o mil.uy. Deben evitarse, por ejemplo, dominios com.uy o com. Cada inciso debe tener un único dominio identificado como gub.uy o mil.uy según corresponda, donde se publique el portal Web institucional, con excepción de los que justifiquen la necesidad de un dominio autónomo, lo que podrá

	efectuarse considerando: funciones y competencias, nivel de aprehensión ciudadana, capacidad de mantenimiento del sitio, disponibilidad de recursos o justificación de la necesidad. Dichas excepciones deberán ser validadas por Agesic. El nombre del dominio deberá seguir los lineamientos detallados en el punto “Nombres de Dominio” del Anexo I del decreto 92/014.
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Accesos a los dominios con su identificación. • Listados de los portales Web que tiene el organismo con dominios y subdominios. • Acceso a los servidores DNS.
Normativa asociada	Decreto 92/014 (Anexo I)
Documentación de apoyo asociada	Anexo III - AIII.6 Guía Interpretación Decreto ciberseguridad – Dominios.
Requisito SC.2	Los portales Web institucionales de Unidades Ejecutoras, aplicaciones, portales y sitios Web correspondientes a proyectos y programas, sitios promocionales y temáticos, incluyendo zonas restringidas de acceso mediante usuario y contraseña disponibles para ciudadanos y funcionarios del organismo (contenidos Web), deberán ser subdominios del dominio del inciso correspondiente.
Objetivo	Optimizar recursos y facilitar el acceso a la información a los ciudadanos.
Alcance	Administración Central
Referencia ISO 27001	N/A
Guía de implementación	<u>Consolidación de dominios</u> En general es deseable que se consoliden todos los dominios de las dependencias de un inciso (Unidades Ejecutoras, Áreas, Oficinas, etc.) en un solo dominio del inciso en un portal orientado a la ciudadanía; sin embargo, es posible asignar un subdominio a estas dependencias. Sin perjuicio de ello, este subdominio debe seguir las mismas recomendaciones de nomenclatura realizadas para el caso de Portales Web Institucionales del Inciso. Lo mismo aplica a las aplicaciones, proyectos, programas, portales promocionales y temáticos que serán subdominios del dominio del inciso. Un ejemplo de subdominio para la Unidad Centralizada de Adquisiciones, dependiente del MEF, sería: uca.mef.gub.uy <u>Necesidad de dominio autónomo (excepción)</u> Los organismos que tengan la necesidad de un dominio autónomo podrán solicitar la excepción argumentando: funciones y competencias, nivel de aprehensión ciudadana, capacidad de mantenimiento del sitio, disponibilidad de

	recursos o justificación de la necesidad. Dichas excepciones deberán ser validadas por Agesic. Se exceptúan a aquellos canales de comunicación que se justifiquen debidamente por su vínculo con la ciudadanía y su carácter público.
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Accesos a los dominios y subdominios con su identificación. • Listados de los portales Web que tiene el organismo con dominios y subdominios. • Acceso a los servidores DNS. • Portales Web.
Normativa asociada	Decreto 92/014 (Anexo I)
Documentación de apoyo asociada	Anexo III - AIII.6 Guía Interpretación Decreto ciberseguridad – Dominios.
Requisito SC.3	El portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos Web que le reporten.
Objetivo	Unificar la forma de referenciar los dominios/subdominios.
Alcance	Administración Central.
Referencia ISO 27001	N/A
Guía de implementación	En todos los casos en que un Inciso o sus unidades ejecutoras dependientes cuenten con varios dominios y/o subdominios, estos deben estar referenciados en el Portal Web del Inciso, de una manera que resulte claro y fácil de encontrar para el ciudadano.
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Accesos a los dominios y subdominios con su identificación. • Listados de los portales Web que tiene el organismo con dominios y subdominios. • Acceso a los servidores DNS. • Portales Web. • Listado de los subdominios en la página institucional del organismo jerarca.
Normativa asociada	Decreto 92/014 (Anexo I)
Documentación de apoyo asociada	Anexo III - AIII.6 Guía Interpretación Decreto ciberseguridad – Dominios.
Requisito SC.4	Los nombres de dominio del organismo o dependencias serán sus iniciales, su acrónimo, o el nombre con el cual se los conoce públicamente. Deberá justificarse que la denominación elegida sea la más representativa.
Objetivo	Establecer un criterio único para nombrar a los dominios/subdominios.
Alcance	Administración Central
Referencia ISO 27001	N/A

Guía de implementación	Ejemplos: a) Por sus iniciales (Ministerio de Salud Pública): www.msp.gub.uy b) Su acrónimo (Ministerio de Desarrollo Social): www.mides.gub.uy c) Nombre con el cual se conoce públicamente y se justifique que sea más representativo que su nombre, acrónimo o iniciales (Presidencia): www.presidencia.gub.uy d) Ejemplo de los subdominios, para una unidad cualquiera (cuyo nombre es "Unidad") dependiente de un ministerio (cuyo nombre es "Ministerio"), el subdominio sería: unidad.ministerio.gub.uy
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Accesos a los dominios con su identificación. • Listados de los portales Web que tiene el organismo con dominios y subdominios. • Acceso a los servidores DNS. • Portales Web.
Normativa asociada	Decreto 92/014 (Anexo I)
Documentación de apoyo asociada	Anexo III - AIII.6 Guía Interpretación Decreto ciberseguridad – Dominios.
Requisito SC.5	**La información de contacto de los responsables de los dominios y subdominios deberá ser comunicada a Agesic y actualizada en períodos de seis meses.**
Objetivo	Asegurar que la información de contacto de los responsables de los dominios y subdominio se encuentre actualizada y comunicada.
Alcance	Administración Central.
Referencia ISO 27001	N/A
Guía de implementación	La comunicación y actualización de información se debe hacer al CERTuy por correo electrónico. Es necesario considerar la caducidad de los sitios para comunicar su baja cuando su contenido ya no sea necesario, de manera de evitar portales huérfanos.
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Proceso de registro y mantenimiento de dominios y subdominios. • Dato de responsable de los dominios y/o subdominios actualizada en la documentación relativa a los dominios y subdominios. • Revisiones y actualizaciones de la información de contacto en el plazo establecido en el procedimiento de mantenimiento de los dominios y subdominios.
Normativa asociada	Decreto 92/014 (Anexo I)
Documentación de apoyo asociada	Anexo III - AIII.6 Guía Interpretación Decreto ciberseguridad – Dominios.
Requisito SC.6	**Establecer acuerdos de no divulgación.**
Objetivo	Proteger la información de la organización.

Alcance	Cualquier organización
Referencia ISO 27001	A.13.2.4
Guía de implementación	<u>Protección de datos</u> Se debe proteger la información la organización de acuerdo con lo establecido en la Ley de Protección de datos personales y acción de habeas data, y Ley de Derecho de acceso a la información pública y sus respectivos decretos reglamentarios. <u>Definición de acuerdos de no divulgación</u> Se deben definir acuerdos de no divulgación para el personal y proveedores, sin perjuicio de definir acuerdos específicos para otras circunstancias que la organización requiera. Para la elaboración de los acuerdos, debe tomarse en cuenta al menos los siguientes puntos: • Definición de la información que debe ser protegida, como, por ejemplo, la información confidencial. • Duración del acuerdo de no divulgación y qué acciones se deben llevar a cabo cuando finaliza un acuerdo. • Responsabilidades y acciones de las partes que firman el acuerdo para evitar la divulgación no autorizada de la información que se pretende proteger. <u>Revisión de los acuerdos</u> Los acuerdos deberían revisarse periódicamente y cuando surgen cambios que influyan en los requisitos anteriormente mencionados.
Administración Central	Los acuerdos de no divulgación se deben definir al menos para personal no presupuestado, siendo deseable su aplicación a todo el personal.
Instituciones de salud	-
Guía de evidencia para auditoría	• Plantillas de Acuerdos de no divulgación (para personal y/o proveedores). • Copias de acuerdos firmados con el personal (selección de muestra aleatoria para el período auditado). • Copias de acuerdos firmados con proveedores (selección de muestra aleatoria para el período auditado). • Procedimiento para la revisión de los acuerdos de no divulgación. • Evidencia de la revisión periódica del contenido de los acuerdos.
Normativa asociada	Ley 18.381: Derecho de acceso a la información pública. Ley 18.331: Protección de datos personales, acción de habeas data.
Documentación de apoyo asociada	Anexo II - AII.2 Compromiso de no divulgación – Proveedores Anexo II - AII.3 Compromiso de no divulgación – Personal
Requisito SC.7	Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su implementación sobre tecnologías que no garanticen dicho requerimiento.

Objetivo	Proteger los correos electrónicos.
Alcance	Administración Central
Referencia ISO 27001	N/A
Guía de implementación	Ubicación en territorio nacional Se pretende que los servidores de correo electrónico pertenecientes al gobierno o Mail Transfer Agent (MTA), o todo aquel que procese correos con dominios gub.uy, se encuentren físicamente implementados dentro del territorio nacional. Esto significa que las interfaces de red que estén conectadas a Internet cuenten con direcciones IP públicas pertenecientes a los rangos asignados a Uruguay. Con esto se busca que los correos electrónicos procesados y almacenados por dichos servidores se encuentren alojados dentro de la jurisdicción de la Republica Oriental de Uruguay. Almacenamiento de los correos electrónicos en territorio nacional Considerando que este requisito también hace referencia al almacenamiento de los correos electrónicos, se debe considerar que cualquier repositorio o medio de almacenamiento en donde existan correos (servidores, respaldos, etc.) se encuentra dentro del alcance de este punto, no permitiéndose por ejemplo realizar ni trasladar respaldos de los mismos fuera del territorio nacional. Este punto también hace referencias a aquellas tecnologías que no permitan cumplir con este requerimiento, como por ejemplo aquellos servicios de correo que estén soportados por infraestructuras Cloud las cuales estén distribuidas por el globo o proveedores que brinden dichos servicios también de forma distribuida dificultando la asociación de una dirección IP a un país en particular.
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Registros MX y whois de las IP de los registros MX. • Infraestructuras Cloud y/o proveedores que brindan este servicio al organismo. • Rango de IP con la que cuentan las interfaces de red que están conectadas a Internet. • Servidores de correo que procesan correos con dominios gub.uy. • Ubicación física de los correos y respaldos. • Acuerdos de niveles de servicio con los proveedores en caso de infraestructura que no esté administrada por el organismo (por ejemplo, Cloud privada).
Normativa asociada	Decreto 92/014 (Anexo II)
Documentación de apoyo asociada	Anexo III - AIII.7 Guía Interpretación Decreto ciberseguridad - Servicios de correo
Requisito SC.8	Garantizar que los correos electrónicos en tránsito entre dos MTAs, o entre un MUA y un MTA, no comprometa la confidencialidad de la información cuando esto sea posible.

Objetivo	Proteger la seguridad de los correos electrónicos, preservando la propiedad de la confidencialidad en los mensajes transmitidos desde y hacia el servidor de correos electrónicos, tanto para aquellas transferencias realizadas entre servidores de correo como las realizadas entre clientes de correo y servidores.
Alcance	Cualquier organización
Referencia ISO 27001	N/A
Guía de implementación	Para poder cumplir con este requerimiento, es necesario implementar protocolos de transferencia seguros que usen algoritmos robustos de cifrado de datos, como lo pueden ser STARTTLS, S/MIME, POP3S, IMAPS, o cualquier nuevo protocolo que brinde tal prestación.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Evidencia de aplicación de los protocolos que usen algoritmos de cifrado de datos. • Archivo de configuración del servidor. • Prueba del cliente de correo utilizados.
Normativa asociada	Decreto 92/014 (Anexo II)
Documentación de apoyo asociada	Anexo III - AIII.7 Guía Interpretación Decreto ciberseguridad - Servicios de correo
Requisito SC.9	**La implementación de canales de comunicación cifrados entre MTA de dominios gubernamentales es obligatoria y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales deberán interrumpir el intento de entrega o recepción de mensajes si este canal cifrado no se puede negociar.**
Objetivo	Lograr que todo correo electrónico intercambiado entre servidores gub.uy se realice únicamente utilizando protocolos seguros, que no estén considerados obsoletos o vulnerables, los cuales hacen uso de cifrado robusto de datos.
Alcance	Administración Central
Referencia ISO 27001	N/A
Guía de implementación	Se deberá configurar reglas de distribución de correos (dentro del software de plataforma utilizado) las cuales establezcan este requerimiento. La forma de realizar esta configuración puede variar entre las diferentes plataformas de correo existentes. El requerimiento de la interrupción de intento de entrega no debe implementarse hasta que Agesic indique, debido a que para habilitar esto es necesario que todos los servidores de correo gubernamentales estén configurados correctamente. Mientras tanto, debe configurarse el canal cifrado como método preferido (no mandatorio). Agesic comunicará de manera oportuna cuando la obligatoriedad de esto deba implementarse.
Administración Central	-
Instituciones de salud	N/A

Guía de evidencia para auditoría	• Proceso o guía para la configuración de los servidores de correo • Configuración de los servidores de correo, configuraciones de reglas de distribución de correos, etc. • Protocolos que se utilizan para el intercambio de correos.
Normativa asociada	Decreto 92/014 (Anexo II)
Documentación de apoyo asociada	Anexo III - AIII.7 Guía Interpretación Decreto ciberseguridad - Servicios de correo
Requisito SC.10	La implementación de canales de comunicación cifrados con protocolos seguros entre MTA de dominios gubernamentales y un MTA de terceros deberá ser el método preferido de comunicación. Cuando el establecimiento de estos canales cifrados no sea posible, se podrá establecer un canal en texto claro.
Objetivo	Lograr que todo correo intercambiado con servidores externos al ámbito gubernamental sea transmitido tratando de conservar la confidencialidad de los datos.
Alcance	Administración Central
Referencia ISO 27001	N/A
Guía de implementación	Siempre que se realice una transferencia de correos con un servidor de correo que no sea gubernamental, o sea, que no pertenezca al dominio gub.uy o mil.uy, se deberá preferir el uso de protocolos seguros para realizarla. Pero debido a que no todos los servidores implementados en Internet soportan esta característica, es necesario que el servidor pueda, en su defecto, realizar la transferencia del mensaje. Para ello y como última opción se podrá realizar el envío del correo sin utilizar cifrado alguno.
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Configuración que indique que MTA se encuentra establecido como método preferido.
Normativa asociada	Decreto 92/014 (Anexo II)
Documentación de apoyo asociada	Anexo III - AIII.7 Guía Interpretación Decreto ciberseguridad - Servicios de correo
Requisito SC.11	La implementación de canales de comunicación cifrados entre MUA y MTA de dominios gubernamentales es mandatoria, y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales no deberán aceptar la descarga o entrega de correos por parte de MUA si este canal cifrado no se puede negociar. Los MTA no deberán aceptar la descarga o consulta de correos electrónicos sobre canales en texto claro.
Objetivo	Asegurar que siempre que un cliente de correo se conecte a un servidor para realizar la descarga o envío de correo electrónico lo pueda hacer únicamente a través de protocolos seguros.
Alcance	Administración Central
Referencia ISO 27001	N/A

Guía de implementación	Es necesario que los servidores únicamente ofrezcan la posibilidad de conexión a través de protocolos seguros y además se debe adecuar la configuración de los clientes de correo para que utilicen los protocolos ofrecidos. El intento de entrega o consulta de correos electrónicos entre clientes de correo y servidores de correo mediante protocolos inseguros deberá ser impedido.
Administración Central	-
Instituciones de salud	N/A
Guía de evidencia para auditoría	• Configuración que indique que MTA se encuentra establecido como método preferido
Normativa asociada	Decreto 92/014 (Anexo II)
Documentación de apoyo asociada	Anexo III - AIII.7 Guía Interpretación Decreto ciberseguridad – Servicios de correo
Requisito SC.12	Los servicios de Webmail deben implementarse sobre el protocolo HTTPS utilizando un certificado de seguridad válido. Cuando la información a transmitir vía email represente un riesgo alto para la organización, se recomienda implementar un modelo de cifrado a nivel de mensaje.
Objetivo	Proteger la confidencialidad de este tramo de la comunicación, entre el navegador del cliente y el servicio Web y para esto se requiere el uso de SSL y la implementación de certificados digitales válidos y emitidos por una Autoridad Certificadora de confianza.
Alcance	Cualquier organización
Referencia ISO 27001	N/A
Guía de implementación	Un servicio de Webmail es un MUA implementado en la Web. Un MUA establece conexiones con el servidor de correo y realiza envío y recepción de mensajes. Además de esto también transmite información hacia el browser del usuario, transmisión que incluye los correos que el usuario recibe y envía. Debe tenerse en cuenta que el servicio de Webmail podría estar implementado en un servidor diferente al servidor de correo y en consecuencia podría llegar a almacenar la información de los correos. Utilizar el protocolo HTTPS y certificados de seguridad válidos, para la implementación de servicios de Webmail Se recomienda implementar un modelo de cifrado a nivel de mensaje para el envío de información de alto riesgo.
Administración Central	No se debe implementar un servicio de Webmail fuera de territorio nacional. Los titulares de cuentas de correo de dominios gubernamentales no podrán acceder a sus cuentas desde servicios Webmail que no sean el provisto por el organismo. Se debe revisar periódicamente que los accesos a las cuentas de correo de dominios gubernamentales no se realicen desde servicios de Webmail externos al organismo (Gmail, Yahoo, Hotmail, etc.).

Instituciones de salud	En caso de transferir datos relacionados a las historias clínicas de los usuarios o cualquier otro dato personal, las instituciones deben asegurarse de que: • Los servidores de correo electrónico y Webmail se encuentren alojados en países que "proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia" en cumplimiento con el artículo 23 de la ley 18.331, o • Que se encuentren amparados por alguna excepción, como la contemplada en el punto 2 del artículo 23: "Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas.". • Además, se debe contemplar lo indicado en el requisito "SO.6 – Respaldar la información y realizar pruebas de restauración periódicas", en el punto Instituciones de salud.
Guía de evidencia para auditoría	• Servicios de Webmail que utiliza la organización, con información sobre dónde se encuentran implementados y sobre qué plataformas (para verificar que no se puede ingresar por http) así como los protocolos implementados (por ejemplo, HTTPS). • Certificados de seguridad válidos (que no sean autofirmados). • Evidencia de que no se puedan chequear las cuentas institucionales desde otros sistemas Webmail (por ejemplo, verificación con el administrador del correo, del log del servidor en busca de entradas desde servicios externos). • Circular o nota donde se indica que está prohibido chequear las cuentas de correo institucionales desde otros servicios de correo. • Chequeo de existencia de reenvío de correos institucionales a otras casillas de correo no pertenecientes al organismo.
Normativa asociada	Decreto 92/014 (Anexo II) Ley 18.331: Protección de datos personales y habeas data
Documentación de apoyo asociada	Anexo III - AIII.7 Guía Interpretación Decreto ciberseguridad - Servicios de correo.
Requisito SC.13	Debe existir segregación a nivel de servicios de información.
Objetivo	Asegurar la protección de la información en las redes.
Alcance	Cualquier organización
Referencia ISO 27001	A.13.1.3
Guía de implementación	Política de segregación de redes Definir una política de segregación de redes donde se contemplen al menos los siguientes puntos: • Segmentación al menos en redes con contacto directo con redes externas y privadas de la organización. • Segregación de las redes en función de grupos de servicios de información o dominios, usuarios y

	sistemas de información, por ejemplo, estableciendo dominios de red separados en función de las unidades organizacionales (RRHH, finanzas, marketing, TI, etc.) o según lo defina la organización. • Definición de los perímetros de cada dominio o segmento mediante, por ejemplo: firewalls o routers de filtrado, definiendo el tráfico por defecto entre segmentos. • Contemplar las redes inalámbricas y evaluar considerarlas como si fuesen conexiones externas para el caso de los entornos que sean sensibles. También sería necesario considerar que las redes inalámbricas estén separadas de las redes internas. • Definición de alertas de tráfico no autorizado. • Alineación con la política y procedimientos de gestión de incidentes y monitoreo. Diagrama de red Se debe contar con diagrama/s de red actualizado/s.
Administración Central	-
Instituciones de salud	Se debe evaluar la necesidad de utilizar segregación para los diferentes servicios, por ejemplo: laboratorio clínico, imagen médica, CTI, entre otros. Se debe considerar especialmente la segregación de la red que contenga componentes que gestionen información y/o intervengan en la prestación de servicios de salud.
Guía de evidencia para auditoría	• Procedimiento para la segregación de las redes. • Diagrama de red detallado indicando la segregación definida en caso de que exista. • Organigrama de la organización donde se pueda identificar la ubicación del rol o función de seguridad de la información y determinar la segregación de funciones/tareas. • Rol o función de administrador de seguridad con descripción de tareas que realiza. • Personal asignado a la administración de la red, al monitoreo y revisión.
Normativa asociada	N/A
Documentación de apoyo asociada	N/A
Requisito SC.14	**Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.**
Objetivo	Mantener la seguridad de la información que se intercambia o transfiere dentro de la organización y con cualquier entidad externa a la misma. Establecer el marco en el cual se intercambiará información desde y con la organización.
Alcance	Cualquier organización
Referencia ISO 27001	A.13.2.1, A.13.2.2, A.13.2.3
Guía de implementación	Política y procedimiento para transferencia de información física y lógica

	Deben establecerse una política, procedimiento y controles que cubran al menos aspectos como: • Procedimientos para transferencia de información a través de cualquier medio de comunicación, incluso teniendo en cuenta el traslado físico de la información. • Medidas de protección al transferir la información contra la intercepción, realización de copias o modificaciones no autorizadas. • Medidas de protección que deben definirse para lograr protección ante software malicioso. • En caso que corresponda, indicar el uso de criptografía. • A nivel de RRHH, se debería incluir en las políticas (y / o generar procedimientos) de sensibilización al personal que indiquen aspectos como evitar mantener conversaciones confidenciales en lugares públicos o mediante canales de comunicación inseguros como podría ser oficinas abiertas, transporte público, restoranes, lugares de reunión, etc. <u>Acuerdos de transferencia segura</u> A nivel de lo que sería la transferencia física de la información, deben establecerse acuerdos de transferencia segura entre la organización y terceras partes que incluya al menos las diferentes responsabilidades durante la transferencia, características de los servicios de mensajería en caso que los hubiere, cómo sería el etiquetado según su clasificación, normas de empaquetado de la información previo a su transferencia, entre otros. Para la transferencia electrónica de información se debe tener presente el requisito “CA.3 Establecer controles criptográficos”.
Administración Central	En cuanto a la mensajería electrónica, es necesario contemplar como mínimo los aspectos establecidos en el Decreto 92/014.
Instituciones de salud	-
Guía de evidencia para auditoría	• Política y procedimientos para la transferencia de información tanto física como electrónica. • Detalle del uso de criptografía. • Muestras de acuerdos o cláusulas de los acuerdos con relación a la transferencia segura de la información. entre la organización y terceras partes. • Detalle de la configuración del correo electrónico.
Normativa asociada	Decreto 92/014
Documentación de apoyo asociada	Anexo I - AI.4 Política de Traslado físico de la información. Anexo I - AI.14 Política de Intercambio de información.
Requisito SC.15	Todo sitio Web que contenga u oficie de enlace a un trámite en línea debe tener un firewall de aplicación Web (Web Application Firewall – WAF).
Objetivo	Aumentar los niveles de seguridad de las aplicaciones y/o portales expuestos a Internet.

Alcance	Cualquier organización.
Referencia ISO 27001	N/A
Guía de implementación	Instalar un WAF delante del sitio Web (por ejemplo, el módulo de Apache mod_security, pudiendo ser cualquier otro WAF). Se recomienda instalar un WAF en producción y otro en pruebas para evitar problemas a la hora del pasaje de la aplicación a producción. En el caso de utilizar mod_security, en los momentos iniciales, luego de su instalación, se recomienda dejarlo en modo "detección" para aprender del tráfico y poder ajustar el WAF a las necesidades del sitio; para luego pasarlo a modo "bloqueo". Se entiende que en producción siempre debería estar en modo "boqueo" para que este cumpla su objetivo.
Administración Central	Todo sitio Web que contenga u oficie de enlace a un trámite en línea debe tener un firewall de aplicación Web (Web Application Firewall - WAF). Se debe crear un procedimiento de reporte mensual al CERTuy sobre estadísticas de la actividad detectada en el WAF. El organismo debe con el CERTuy en la centralización de registros de WAF a nivel nacional.
Instituciones de salud	Se recomienda contar con un procedimiento de reporte mensual al CERTuy o equipo de respuesta que corresponda, sobre estadísticas de la actividad detectada en el WAF. Se sugiere que la institución colabore con el CERTuy o equipo de respuesta que corresponda, en la centralización de registros de WAF a nivel nacional.
Guía de evidencia para auditoría	• Configuración de WAF. • Reportes realizados al CERTuy o equipo de respuesta correspondiente.
Normativa asociada	N/A
Documentación de apoyo asociada	N/A

4.11 Adquisición, desarrollo y mantenimiento de los sistemas

Requisito AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.
Objetivo	Garantizar que la seguridad de la información forma parte de los sistemas de información en todo el ciclo de vida de los proyectos y en las adquisiciones.
Alcance	Cualquier organización
Referencia ISO 27001	A.14.1.1, A.14.2.1, A.14.2.3, A.14.2.7, A.14.2.8, A.14.2.9
Guía de implementación	Requisitos de seguridad de la información en los proyectos Dentro de la metodología de gestión de proyectos de sistemas de información, debe contemplarse los requisitos de seguridad de la información, formando parte de la especificación de requisitos para un nuevo sistema o bien modificaciones en los

	sistemas existentes. Es recomendable establecer los requisitos de seguridad en etapas tempranas para lograr sistemas más eficaces y eficientes. Criterios de aceptación Dentro de los criterios de aceptación de productos, se deben incluir los criterios de cumplimiento con requisitos de seguridad de la información de la organización. Desarrollo seguro Deben establecerse pautas o lineamientos para el desarrollo seguro donde se defina o se requiera el uso de una metodología de desarrollo de software que tenga como objetivo producir código seguro en forma consistente. La metodología de desarrollo debe abordar entre otros, los siguientes aspectos: • Criterios de aceptación de diseño, pruebas y documentación. • Participación del usuario directamente o mediante algún rol que los represente. • Plan de pruebas con participación usuaria. • Controles de seguridad que sean necesarios (por ejemplo, análisis de riesgo de amenazas, revisiones de código, etc.). • Lineamientos de seguridad de la información en el ciclo de vida del desarrollo de software. • Lineamientos de codificación para el lenguaje de desarrollo utilizado. En este punto deberán considerarse aspectos como: - Niveles mínimos de documentación requerida. - Requerimientos de prueba obligatorios. - Cómo realizar comentarios entre código y cuál sería el estilo de comentarios preferidos. - Manejo de excepciones. - Método para nombramiento de variables, funciones, clases y tablas. - El código fuente debería ser fácil de mantener y legible. Control de versiones Se debe contar con mecanismos para el control de versiones y revisión de código (por ejemplo, Subversion, SourceSafe, CVS, ClearCase, etc.) Desarrollo subcontratado Si el desarrollo se realiza en forma subcontratada, la organización debe acordar con los proveedores el

	cumplimiento de las normas de desarrollo seguro que se hayan definido. <u>Adquisición de productos</u> En el caso de adquisición de productos, los contratos con los proveedores deben incorporar los requisitos de seguridad que sean necesarios. En caso de que esos requisitos de seguridad no puedan ser satisfechos, debe considerarse el riesgo generado por esta causa y evaluar si realmente se va a adquirir el producto.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Pautas de desarrollo seguro. • Metodología de gestión de proyectos. • Metodología de desarrollo que incluya aspectos de seguridad y evidencia de su revisión periódica. • Lista de proyectos (desarrollado internamente o adquirido a un tercero) durante el período auditado. • Listado de aplicaciones. • Especificación de requerimientos para algunos proyectos seleccionados como muestra, donde se incluyan los requerimientos relativos a seguridad de la información. • Trazabilidad requerimiento – persona de contacto. • Documentación generada en relación con los proyectos de desarrollo. • Muestra de versionado de archivos para el período auditado. • Política de gestión de cambios. • Procedimiento de gestión de cambios. • Detalle de la herramienta (si existiera) que asiste en la gestión de los cambios. • Listado de solicitudes de cambios en el período auditado.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.22 Política de Gestión de cambios. Anexo II - AII.5 Requerimientos de Seguridad de la información para adquisición de soluciones.

4.12 Relación con proveedores

Requisito RP.1	Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.
Objetivo	Contar con acuerdos de niveles de servicios que permitan nivelar las expectativas y responder con la calidad establecida y en los tiempos establecidos.
Alcance	Cualquier organización
Referencia ISO 27001	A.14.2.7, A.15.2.1
Guía de implementación	<u>Soporte, mantenimiento y régimen de cobertura</u> Todo sistema, servicio y equipamiento crítico del centro de datos debe contar con soporte de mantenimiento y recambio de partes o, en su defecto, con un plan acción en caso de falla. Se debe establecer el régimen de cobertura para los servicios críticos de acuerdo a las necesidades de la organización. La administración de infraestructura del centro de datos requiere atención en modalidad 7x24 (o la que mejor se adapte a las necesidades del negocio). <u>Acuerdos de nivel de servicio</u> Muchas veces las organizaciones no tienen la capacidad operativa para cubrir este servicio por lo que delegan o comparten la operación del centro de datos a proveedores. Es importante firmar con los proveedores acuerdos de niveles de servicio que pauten el cumplimiento de tiempos de respuesta, estipulados según las necesidades de negocio, así como el aseguramiento de la disponibilidad comprometida de los servicios del centro de datos. <u>Tiempos de respuesta</u> También es necesario tener acuerdos que aseguren los tiempos de respuesta para aquellos componentes que por su complejidad no puedan ser redundantes pero que, por su criticidad, su falla pueda provocar disrupción de servicios u otros daños.
Administración Central	Se debe contar con cobertura en un régimen 7x24x365 para los componentes críticos del centro de datos.
Instituciones de salud	-
Guía de evidencia para auditoría	• Listado de proveedores de servicios críticos. • Política de relacionamiento con proveedores. • Procedimiento de gestión de proveedores. • Contrato con proveedores y acuerdos de nivel de servicio (SLA). • Registro de las mediciones del desempeño, acciones de mejora para ajustar el servicio, llevadas a cabo durante el período auditado. • Muestra de registro de incidentes con proveedores con tiempo de respuesta y resolución.
Normativa asociada	Decreto 92/014 (Anexo III)

Documentación de apoyo asociada	Anexo I - AI.26 Política de Relacionamiento con proveedores. Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.
Requisito RP.2	Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
Objetivo	Establecer y asegurar el cumplimiento de los términos y condiciones de seguridad de la información de los contratos y acuerdos de nivel de servicio con los proveedores. Garantizar que los incidentes y problemas de seguridad de la información se manejan de forma adecuada. Asegurar que se gestiona adecuadamente la seguridad de la información frente a cambios en los servicios de los proveedores.
Alcance	Cualquier organización
Referencia ISO 27001	A.15.2.1, A.15.2.2
Guía de implementación	Se debe establecer un procedimiento de supervisión de los niveles de desempeño del servicio, en concordancia con los SLAs y los contratos. Debe evaluarse la posibilidad de realizar auditorías de los proveedores y, en función de sus resultados, reevaluar riesgos frente a cambios en los servicios de los proveedores.
Administración Central	-
Instituciones de salud	Cuando se adquieran dispositivos médicos, validar que incorporen los últimos controles de seguridad ciberseguridad. Además, se deben establecer los roles y responsabilidades relacionados con las actualizaciones, parches, administración de contraseñas, acceso remoto, etc., para garantizar la ciberseguridad de los productos o servicios.
Guía de evidencia para auditoría	• Política de relación con proveedores. • Lista de proveedores de servicios críticos. • Acuerdos de Nivel de Servicio (SLA). • Contrato con los proveedores. • Registro de revisiones regulares de los SLA y contratos con proveedores de servicios.
Normativa asociada	N/A
Documentación de apoyo asociada	Anexo I - AI.26 Política de Relación con proveedores

4.13 Gestión de incidentes

Requisito GI.1	Planificar la gestión de los incidentes de seguridad de la información.
Objetivo	Prevenir y mitigar el impacto de los incidentes de seguridad de la información.
Alcance	Cualquier organización.
Referencia ISO 27001	A.16.1.1
Guía de implementación	<u>Política de gestión de incidentes</u> Se debe definir una política de gestión de incidentes de seguridad de la información. <u>Responsables de la gestión de incidentes</u> Asimismo, se deben definir las responsabilidades para la gestión de los incidentes de seguridad de la información de la organización y del personal. <u>Procedimientos de gestión de incidentes</u> Es recomendable definir procedimientos que aborden al menos, los siguientes aspectos: • Detección de incidentes de seguridad (por ejemplo, mediante el monitoreo de sensores, WAF, etc.). • Registro de los incidentes. • Reporte de los incidentes. • Clasificación de incidentes (cuando se asigne una clasificación se debe tener en cuenta el riesgo e impacto asociado). • Evaluación y decisión sobre los incidentes de seguridad. • Respuesta a incidentes. • Seguimiento y cierre de incidentes (incluye elaboración de informes definitivos e implementación de medidas correctivas). <u>Mejora continua</u> Se deben tomar en cuenta las actividades necesarias para el proceso de mejora continua de la gestión de incidentes, tomando como base lecciones aprendidas e información que surge del registro de los incidentes, de las actividades realizadas y de sus respuestas.
Administración Central	Planificar la gestión de los incidentes de seguridad de la información de acuerdo a los lineamientos establecidos por el CERTuy.
Instituciones de salud	La política de gestión de incidentes de seguridad de la información y/o el plan de gestión de incidentes debe contemplar el equipamiento médico.
Guía de evidencia para auditoría	• Política de gestión de incidentes de seguridad de la información.

	• Procedimientos existentes para la gestión de incidentes de seguridad de la información. • Listado de incidentes del período auditado. • Mesa de ayuda o mesa de servicios formalmente constituida. • Herramienta de software de apoyo a la gestión de incidentes. • Responsables definidos para la gestión de incidentes.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	Anexo I - AI.2 Política de Gestión de incidentes de seguridad de la información. Anexo III - AIII.3 Clasificación de incidentes. Anexo III - AIII.4 Guía de procesos en gestión de incidentes.
Requisito GI.2	Contar con mecanismos que permitan evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.
Objetivo	Lograr identificar el impacto y alcance de un evento y determinar si es un incidente.
Alcance	Cualquier organización
Referencia ISO 27001	A.16.1.4
Guía de implementación	En función de la política de gestión de incidentes de seguridad de la información y de los procedimientos, cada punto de contacto debería evaluar cada evento de seguridad siguiendo la escala establecida. La evaluación y decisión de la clasificación del evento, podría enviarse al CERTuy o equipo de respuesta que corresponda para su confirmación o reevaluación. Se debe contar con un registro de las evaluaciones y decisiones tomadas para tener una futura referencia y verificación.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Política de gestión de incidentes de seguridad de la información. • Pautas o procedimiento para la clasificación de los posibles incidentes. • Procedimiento de reporte de incidentes de seguridad de la información. • Listado de incidentes de seguridad de la información del período auditado. • Mecanismos y procedimientos empleados para el registro de incidentes de seguridad. • Detalle de la información o consultas enviadas al CERTuy o equipo de respuesta correspondiente.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	Anexo I - AI.2 Política de Gestión de incidentes de seguridad de la información. Anexo III - AIII.3 Clasificación de incidentes.

Requisito GI.3	Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy o equipo de respuesta externo correspondiente.
Objetivo	Asegurar que los incidentes de seguridad de la información se reportan a las personas adecuadas y en forma consistente de acuerdo a la política de gestión de incidentes. Determinar si es un incidente de seguridad informática a reportar al CERTuy o equipo de respuestas externo.
Alcance	Cualquier organización
Referencia ISO 27001	N/A
Guía de implementación	Se deben definir los canales de gestión de incidentes de seguridad de la información internamente en la organización. El RSI o quien este determine debe ser el punto de contacto ante incidentes detectados o sospechados. Eventualmente, el RSI podría designar a alguien para que cumpla este rol. Es recomendable definir procedimientos para un adecuado reporte de los incidentes que aplique a la organización y sus proveedores, indicando claramente responsables, el orden de los pasos, puntos de contacto y las herramientas a utilizar.
Administración Central	Siempre debe contactarse al CERTuy por las vías de comunicación publicadas en su sitio Web: www.cert.uy. Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy.
Instituciones de salud	En función a lo establecido en el Compromiso de Uso de la Red Salud, V. Obligaciones del Usuario, punto c) Obligación de reportar incidentes: “Los Usuarios deberán reportar ante Agesic cualquier incidente que represente un riesgo directo o indirecto a la Red Salud o cualquiera de sus componentes”. La dirección de correo para reportar incidentes de seguridad de la información para instituciones de Salud es: hcen@salud.uy, salvo que se establezca otro mecanismo.
Guía de evidencia para auditoría	• Política de gestión de incidentes de seguridad de la información. • Procedimiento para el reporte de incidentes de seguridad de la información. • Lista de incidentes de seguridad de la información reportados al CERTuy o equipo de respuesta correspondiente con detalle de seguimiento, fecha y hora de registro.
Normativa asociada	Decreto 451/009 Decreto 452/009
Documentación de apoyo asociada	Anexo I - AI.2 Política de Gestión de incidentes de seguridad de la información.
Requisito GI.4	Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.
Objetivo	Lograr que todos los incidentes sean registrados oportunamente para evaluarlos, estudiarlos, contar con estadísticas y tomar las acciones necesarias en forma rápida y efectiva siguiendo los procedimientos establecidos.

Alcance	Cualquier organización
Referencia ISO 27001	A.16.1.2, A.16.1.3
Guía de implementación	Debe definirse un procedimiento para el reporte de incidentes confirmados o sospechados, alineado con la política de gestión de incidentes y difundirlo a todo el personal. Los reportes de incidentes deben quedar registrados y es recomendable utilizar herramientas automatizadas para facilitar su gestión. Es necesario concientizar al personal en qué tipos de eventos son los que debe reportar y registrar, así como difundir los mecanismos para hacerlo. Debe ser contemplado el reporte anónimo para los casos que tengan una sensibilidad especial en su tratamiento y contenido.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Política de gestión de incidentes de seguridad de la información. • Procedimiento de reporte de incidentes de seguridad de la información. • Procedimiento de clasificación de incidentes. • Lista de incidentes reportados en el período auditado.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	Anexo I - AI.2 Política de gestión de incidentes de seguridad de la información. Anexo III - AIII.4 Guía de procesos en gestión de incidentes.
Requisito GI.5	**Responder ante incidentes de seguridad de la información.**
Objetivo	Lograr acciones de respuestas coordinadas, rápidas y efectivas ante los incidentes de seguridad de la información. Asegurar que puede reanudar el nivel de seguridad normal para posteriormente dar comienzo a la recuperación.
Alcance	Cualquier organización
Referencia ISO 27001	A.16.1.5, A.16.1.7
Guía de implementación	Plan y/o procedimiento de respuesta Se debe definir un plan y/o procedimiento de respuesta ante incidentes de seguridad de la información basados en la política de gestión de incidentes de seguridad de la información. Se debe informar al personal periódicamente sobre cómo proceder ante incidentes de seguridad de la información. El plan y/o procedimiento de respuesta debe estar alineado al plan de contingencia y recuperación. Este debe contemplar al menos: • Metodología para recolectar la evidencia de forma tan rápida como sea posible luego de ocurrido el incidente. • Responsables de la respuesta a incidentes de seguridad de la información.

	• Registro de las actividades de respuesta. • Informes a las Gerencias involucradas. • Actividades de análisis forense de seguridad de la información (si corresponden) y recopilación de evidencia • Se deben evaluar los casos en los que corresponda escalar, teniendo en cuenta activos afectados, criticidad y severidad. • Participación del CERTuy o equipo de respuesta que corresponda. • Sistematizar lecciones aprendidas para reducir la probabilidad y/o el impacto ante incidentes similares en el futuro. Se deberían determinar las responsabilidades por la sistematización de las lecciones aprendidas de forma tal que sean sustentables en el tiempo para la organización. Las lecciones aprendidas sobre incidentes pueden ser utilizadas en las actividades de concientización y capacitación en seguridad de la información, considerando los aspectos de confidencialidad que sean necesarios. • La actualización de los planes de respuesta basada en lecciones aprendidas. • Determinar las acciones para contener los incidentes como, por ejemplo, la realización de un análisis para definir si es conveniente la desconexión de los sistemas en peligro o continuar funcionando con la posibilidad de sufrir daños adicionales. • Determinar las pruebas al plan y/o procedimiento de respuesta, su periodicidad y registrarlas. <u>Registro de las actividades de respuesta</u> Se debe contar con un registro de todas las actividades de respuesta. El registro puede ser manual, por ejemplo, mediante la utilización de plantillas de documentos o planillas de cálculo o bien contar con una herramienta automatizada para este fin. El registro es necesario para determinar, por ejemplo, incidentes recurrentes y aquellos que generan más impacto, de forma tal que soporte la toma de decisiones.
Administración Central	-
Instituciones de salud	El plan de gestión de incidentes debe contemplar el equipamiento médico.
Guía de evidencia para auditoría	• Política de gestión de incidentes de seguridad de la información. • Plan de respuesta a incidentes de seguridad de la información. • Procedimiento de respuesta a incidentes de seguridad de la información. • Registro y seguimiento de los incidentes de seguridad de la información para el período auditado.

	• Evidencia de la comunicación al CERTuy o equipo de respuesta correspondiente. • Evidencia de la respuesta del CERTuy o equipo de respuesta correspondiente.
Normativa asociada	Decreto 451/009 Decreto 452/009
Documentación de apoyo asociada	Anexo I - AI.2 Política de gestión de incidentes de seguridad de la información. Anexo III - AIII.4 Guía de procesos en gestión de incidentes.
Requisito GI.6	**Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.**
Objetivo	Lograr que la organización identifique y capitalice las lecciones aprendidas luego de ocurrido un incidente retroalimentando la gestión de riesgos y los controles implementados.
Alcance	Cualquier organización.
Referencia ISO 27001	A.16.1.6
Guía de implementación	• La organización debe ser capaz de lograr una adecuada evaluación de daños (imagen, económicos, operativos, legales, etc.) conjuntamente con una evaluación de costo y esfuerzo para la recuperación. • En caso de que corresponda, se debe ejecutar el plan de recuperación y contingencia. • Se debe realizar un análisis post-incidente que le permita a la organización conocer las causas y rescatar lecciones aprendidas que permitan mejorar los controles existentes. Dicho análisis debe retroalimentar la gestión de riesgos. • Es deseable contar con un repositorio de lecciones aprendidas que pueda ser consultado por los actores claves de la organización. • Una vez entendida la causa raíz del incidente y analizada sus lecciones aprendidas se deberán implementar las acciones de remediación que se entiendan pertinentes.
Administración Central	En particular, se debe priorizar recuperarse de los incidentes de seguridad informática que afecten activos de información críticos del Estado.
Instituciones de salud	Estos mecanismos deben incluir los procesos y procedimientos para recomponer la normal operativa de la institución; incluyendo entre otros, sistemas necesarios para la normal operación con HCEN y todo aquel sistema, proceso, etc. requerido para la normal operativa de la institución.
Guía de evidencia para auditoría	• Informe de evaluación de daños. • Informe de lecciones aprendidas. • Repositorio de lecciones aprendidas.
Normativa asociada	Decreto 451/009
Documentación de apoyo asociada	N/A

4.14 Continuidad de las operaciones

Requisito CO.1	Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos.
Objetivo	Garantizar el normal funcionamiento de los centros de datos y operaciones.
Alcance	Cualquier organización.
Referencia ISO 27001	A.11.1.4, A.17.2.1
Guía de implementación	Para la implementación de controles de acceso físico a los centros de datos y áreas relacionadas, se puede tomar como base el decreto 92/014. <u>Suministro de energía</u> • Se debe contar con un sistema generador de energía eléctrica con capacidad suficiente para abastecer todo el centro de datos. • Se debe contar con sistemas redundantes de alimentación ininterrumpida. • Se deben implementar unidades de distribución de energía (PDU) redundantes. • Para energizar los racks se deben implementar circuitos eléctricos redundantes de tal manera que el fallo de uno de ellos no afecte a más de un rack. Los centros de datos de la organización deben contar con generador de energía eléctrica, sistemas redundantes de alimentación ininterrumpida, PDU y circuitos eléctricos redundantes. Los cortes de energía en un centro de datos no solo impiden la continuidad de los servicios, sino que el apagado no programado del equipamiento puede ocasionarles daños irreversibles. Por esto es necesario tener esquemas redundantes de energía eléctrica para el centro de datos. En Uruguay contamos con un único proveedor de energía eléctrica (UTE) por lo que contar con un respaldo de energía implica tener un generador de energía propio (o arrendado de uso exclusivo). Este generador debe ser dimensionado para poder abastecer la totalidad de carga eléctrica del centro de datos. Contar con un generador de energía no es suficiente, pues en caso de requerir su uso se produce interrupción de energía eléctrica entre que se detecta el corte en el suministro de la red y se enciende el generador. Es por esto que es necesario contar, además, con sistemas de UPS (sistema de energía ininterrumpido) a baterías que puedan soportar la carga de todo el centro de datos durante estos cortes.

	Actualmente casi todos los activos de un centro de datos, como servidores, switches, routers o firewalls, cuentan con alimentación redundante de energía eléctrica. Esto es porque es común que falle una línea de energía y los equipos están pensados para no interrumpir su funcionamiento en caso de que alguna falle. Para poder cumplir con este fin, es necesario que a este equipamiento le lleguen dos líneas eléctricas independientes. Para proteger además los sistemas críticos de los centros de datos que no tengan doble fuente de energía, existen en el mercado dispositivos que se conectan a las dos líneas eléctricas y que entregan una sola fase. Finalmente, para minimizar el impacto de fallas eléctricas, se solicita que las acometidas eléctricas desde el tablero general a cada rack sean exclusivas para ellos. <u>Climatización</u> • El sistema de climatización debe contar con una redundancia que garantice los niveles de temperatura y humedad relativa en caso de falla o mantenimiento de uno de sus componentes. • Los sistemas de aire acondicionado deben estar diseñados para un funcionamiento continuo 7 días/24 horas/365 días/año. El sistema de climatización debe ser alimentado por el generador de energía eléctrica. Los sistemas de acondicionamiento térmico deben ser redundantes, pues en caso que fallen la temperatura del centro de datos puede alcanzar valores no deseados que provoque desde la falla en el equipamiento que cause la pérdida de su garantía, hasta un posible incendio.
Administración Central	-
Instituciones de salud	Se deben tomar las medidas necesarias para asegurar la disponibilidad del suministro de energía eléctrica de los equipos de áreas críticas o que cumplan funciones críticas que se encuentren fuera del centro de datos.
Guía de evidencia para auditoría	• Generador de energía. • UPS. • Líneas eléctricas independientes. • Control del tablero (exclusividad para cada rack de las acometidas eléctricas desde el tablero general). • Sistema de aire acondicionado.
Normativa asociada	Decreto 92/014 (Anexo III).
Documentación de apoyo asociada	Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.
Requisito CO.2	Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia.

Objetivo	Asegurar que la infraestructura de redes del centro de datos no tenga puntos únicos de falla, es decir, que la operativa del centro de datos pueda continuar aun ante la caída de un activo de red.
Alcance	Cualquier organización.
Referencia ISO 27001	A.17.2.1
Guía de implementación	Se deben implementar mecanismos que aseguren el adecuado funcionamiento de la red ante un posible fallo de equipamiento crítico de telecomunicaciones. Esto puede resolverse mediante redundancia, protocolos, etc. Este requisito ayuda a evitar los puntos únicos de falla en la red o componentes de red, es decir, que la falla de un dispositivo afecte a una gran parte de la red (incluidos los servicios críticos). Hay varias formas de implementar redundancia. Se recomienda el uso de soluciones automáticas que no requiera acciones manuales por parte de un operador para lograr la recuperación del servicio. El objetivo es que, en caso de falla, las aplicaciones críticas del negocio puedan continuar funcionando y que estén documentados todos los procedimientos necesarios para continuar operando.
Administración Central	-
Instituciones de salud	Se deben tomar las medidas necesarias para asegurar la disponibilidad de los equipos de áreas críticas o que cumplan funciones críticas que se encuentren fuera del centro de datos.
Guía de evidencia para auditoría	• Plan de continuidad de las operaciones. • Evidencia de las pruebas realizadas al plan en el período auditado (resultados de las pruebas, aprobaciones requeridas, actividades correctivas y de mejora continua). • Sitio de contingencia y facilidades operativas de contingencia.
Normativa asociada	Decreto 92/014
Documentación de apoyo asociada	Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.
Requisito CO.3	**Establecer los medios necesarios para garantizar la continuidad de las operaciones.**
Objetivo	La organización debe brindar los recursos necesarios a las áreas encargadas de gestionar la continuidad para lograr hacer frente y/o estar preparada para situaciones adversas o crisis que puedan afectar la continuidad de las operaciones.
Alcance	Cualquier organización
Referencia ISO 27001	N/A
Guía de implementación	Para el cumplimiento del requisito, la Dirección debería: • Proveer los recursos humanos y materiales necesarios para la gestión de la continuidad en función de la planificación realizada por el área encargada de gestionar la continuidad operativa. • Apoyar la generación del plan de continuidad de las operaciones y de recuperación en caso de desastres

	• Facilitar las tareas de planificación de la continuidad. • Facilitar y promover la realización de las pruebas de continuidad. • Promover el registro de las actividades de pruebas de continuidad operativa y establecer espacios de retroalimentación entre las áreas encargadas de gestionar la continuidad para generar lecciones aprendidas y mejorar los planes.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Planificación anual en tareas de contingencia aprobada por la Dirección.
Normativa asociada	Decreto 452/009
Documentación de apoyo asociada	N/A
Requisito CO.4	Planificar la continuidad de las operaciones y recuperación ante desastres.
Objetivo	Preparar a la organización ante eventos anormales, disruptivos o desastres que puedan afectar sus operaciones, en principio, relacionadas a trámites en línea.
Alcance	Cualquier organización
Referencia ISO 27001	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
Guía de implementación	<u>Planificación, Políticas y procedimientos</u> El objetivo de la planificación de la continuidad es mantener las operaciones de un negocio en caso de una situación de emergencia. El objetivo del equipo dedicado a planificar la continuidad de las operaciones es diseñar políticas, procesos, procedimientos y un plan de contingencia y recuperación para que cualquier evento potencialmente disruptivo tenga el menor impacto posible en el negocio. La meta de un plan de contingencia y recuperación es mantener operativos aquellos procesos de negocio críticos con infraestructura y/o capacidades reducidas, limitadas. La capacidad de continuidad de una organización permite mantener los procesos críticos funcionando y a la vez gestionar las actividades de restauración y recuperación usando el plan de recuperación ante desastres. Dentro de la planificación de la continuidad operativa, se debe considerar la continuidad de la gestión de la seguridad de la información en situaciones de crisis o desastres. Esto implica que los planes deben incluir los requisitos de seguridad de la información. Estos requisitos pueden abordarse en el primer punto mencionado en la metodología (conocimiento de los procesos críticos del negocio y su impacto en el negocio) y deben explicitarse en los planes.

	<u>Metodología para la planificación de la continuidad operativa</u> Para cumplir con estas premisas, la organización debería contar con una metodología para la planificación de la continuidad operativa que incluya al menos: • Conocimiento de los procesos críticos y su impacto en el negocio (análisis BIA). • Análisis de riesgos que pueden afectar los procesos críticos. • Análisis del negocio desde el punto de vista de una crisis o un evento disruptivo que afecte los procesos críticos. • Contar con un equipo para definir las políticas, planes, procesos y procedimientos de contingencia y recuperación. • La conformación del equipo encargado de definir el plan de contingencia y recuperación (con aprobación de la Dirección). • Conocimiento de los aspectos normativos que afectan a la organización. <u>Plan de contingencia y recuperación</u> Una vez analizados los aspectos anteriormente mencionados, la organización debería confeccionar formalmente un plan de contingencia y recuperación. <u>Pruebas al plan de contingencia y recuperación</u> Se debería establecer también un plan de pruebas al plan de contingencia y recuperación, con una frecuencia al menos anual. Se debe tener en cuenta la incorporación de los proveedores de servicios críticos para la realización del plan y pruebas de contingencia y recuperación. <u>Capacitación al personal</u> Se debería también planificar la capacitación del personal con relación a la continuidad operativa. <u>Comunicación</u> Se debería establecer una estrategia de comunicación a todo el personal interno y externo involucrado en caso de circunstancia que requiera la activación del plan de continuidad.
Administración Central	-
Instituciones de salud	Se debe establecer al menos algún mecanismo de contingencia en caso de indisponibilidad de los sistemas de HCE propios para lograr la consulta a la historia clínica de los usuarios. Se recomienda considerar todos los procesos y equipamiento crítico relacionados con la asistencia de los usuarios.

Guía de evidencia para auditoría	• Plan de contingencia y recuperación de las operaciones. • Plan de recuperación ante desastres. • Plan de pruebas del plan de contingencia y recuperación. • Resultados de las pruebas realizadas al plan en el período auditado (resultados, aprobaciones requeridas, actividades correctivas y de mejora continua). • Sitio de contingencia y facilidades operativas de contingencia. • Evidencia de capacitaciones realizadas sobre continuidad operativa.
Normativa asociada	Decreto 452/009 Decreto 92/014
Documentación de apoyo asociada	Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.
Requisito CO.5	Definir las ventanas de tiempo soportadas para la continuidad de las operaciones.
Objetivo	Definir métricas básicas para planificar la continuidad de las operaciones.
Alcance	Cualquier organización.
Referencia ISO 27001	N/A
Guía de implementación	En el marco de la planificación de la continuidad operativa y del impacto en el negocio, una vez que se identifican los procesos críticos de la organización, es necesaria la definición de al menos tres métricas para cada unidad de negocio, que apoyan a la definición de las estrategias de continuidad y recuperación: • MTD: Maximum tolerable downtime o tiempo de inactividad máximo tolerable. • RTO: Recovery time objective o tiempo objetivo de recuperación. • RPO: Recovery point objective o punto objetivo de recuperación. La definición de estas métricas apoyará a la definición de la continuidad operativa de la organización y será punto de partida para la definición de los planes de recuperación. Estas métricas deben tenerse en cuenta al momento de la prueba de los planes.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Plan de continuidad de las operaciones. • Plan de recuperación ante desastres.
Normativa asociada	Decreto 452/009 Decreto 92/014
Documentación de apoyo asociada	Anexo III - AIII.5 Guía Interpretación Decreto ciberseguridad - Centros de datos.
Requisito CO.6	Definir los mecanismos de comunicación e interlocutores válidos.

Objetivo	Difundir y comunicar la situación de crisis o incidentes que afectan a la ciberseguridad de la organización, a través de interlocutores formalmente autorizados.
Alcance	Cualquier organización
Referencia ISO 27001	N/A
Guía de implementación	<u>Plan de comunicaciones</u> Con motivo de informar a las partes interesadas (población en general, clientes, proveedores, prensa, etc.) sobre situaciones de crisis o incidentes que afectan la ciberseguridad, la planificación de las comunicaciones hacia el exterior de una organización implica definir un proceso detallado, así como los responsables de realizar las comunicaciones. Se debe definir un plan de comunicaciones y procedimientos asociados, además de contar con un equipo de comunicaciones ante crisis con responsabilidades asignadas, que se encargará de definir el plan de acción según la situación y seleccionar el vocero principal. El personal debe conocer quién es el vocero autorizado y la vía para contactarlo. Dentro de la planificación de las comunicaciones, se deben abordar ciertos aspectos como: • Evaluación del evento o del incidente (qué ocurrió, cuándo, dónde, qué acciones se están tomando, etc.) • Notificación (al vocero del equipo de comunicaciones). • Determinar el nivel de comunicación requerido (alto, medio, bajo, por ejemplo) y elaborar los mensajes necesarios. • Aprobar y difundir los mensajes (por la Dirección o área competente que se determine). • Monitoreo de las comunicaciones (revisar la cobertura que los medios de comunicación han realizado con la información proporcionada sobre la crisis). • Se considera componer la reputación de la organización luego de un evento disruptivo que provoque daños a la imagen organización. <u>Pruebas al plan de comunicaciones</u> El plan de comunicaciones debe probarse periódicamente en escenarios en conjunto con el plan de contingencia y recuperación. <u>Equipo de comunicaciones</u> La definición del equipo de comunicaciones debe figurar o referenciarse en el plan de contingencia y recuperación.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Plan de contingencia y recuperación. • Plan de comunicaciones ante crisis.

Normativa asociada	N/A
Documentación de apoyo asociada	N/A

4.15 Cumplimiento normativo

Requisito CN.1	Cumplir con los requisitos normativos.
Objetivo	Asegurar el cumplimiento normativo relacionado con la seguridad de la información y con los requisitos de seguridad.
Alcance	Cualquier organización.
Referencia ISO 27001	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
Guía de implementación	La Dirección debe velar por la identificación y documentación de los requisitos normativos relevantes que afectan a la organización, relacionados a seguridad de la información y ciberseguridad, protección de datos personales, entre otras. Tener en cuenta, además, el cumplimiento de los requisitos de derecho de propiedad intelectual y uso de productos de software patentados.
Administración Central	-
Instituciones de salud	Las instituciones de salud deben cumplir con lo establecido en el decreto de HCEN N° 242/2017 el cual, entre otras disposiciones, establece temas relacionados a seguridad. Asimismo, se debe velar por el cumplimiento de lo establecido en la ley 18.335 sobre derechos y obligaciones de pacientes y usuarios de los servicios de salud, la ley 19.286 código de ética médica y secreto profesional.
Guía de evidencia para auditoría	• Resolución con la adopción de la política de seguridad de la información. • Planilla de cumplimiento y Plan de acción (Decreto 092/014). • Registro de base de datos (Protección de datos, Derecho de acceso a la información pública).
Normativa asociada	Decreto 452/009 Decreto 451/009 Decreto 92/014 Ley 18.331: Protección de datos personales y habeas data Ley 18:381: Derecho de acceso a la información pública Ley 19.286: Código de ética médica Leyes que declaren secreta información (secreto tributario, secreto estadístico, secreto bancario, secreto profesional, etc.)
Documentación de apoyo asociada	Anexo II - AII.4 Planilla de cumplimiento y plan de acción - Decreto 92/014
Requisito CN.2	Realizar auditorías independientes de seguridad de la información.
Objetivo	Asegurar la conveniencia, adecuación y eficacia continua de la gestión de la seguridad de la información en la organización de acuerdo al presente marco.
Alcance	Cualquier organización

Referencia ISO 27001	A.18.2.1
Guía de implementación	Es recomendable designar un equipo interno de la organización que no pertenezca al área de TI (por ejemplo, auditoría interna) o externo (por ejemplo, una firma consultora), con las capacidades y habilidades necesarias para planificar, ejecutar y realizar seguimiento del sistema de gestión de seguridad de la información (SGSI). El seguimiento del SGSI debe contemplar actividades de control interno para verificar el cumplimiento de las políticas y procedimientos relacionados. La revisión debe incluir oportunidades de evaluación para la mejora y la necesidad de cambios en el enfoque de seguridad, incluyendo la política y los objetivos de control. Estas revisiones deben realizarse en el marco de la presente guía y en forma periódica.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Informes de revisiones independientes de seguridad de la información. • Seguimiento realizado por la organización para eliminar las observaciones de las revisiones realizadas en forma independiente.
Normativa asociada	N/A
Documentación de apoyo asociada	Marco de Ciberseguridad
Requisito CN.3	**Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades.**
Objetivo	Conocer y mitigar las vulnerabilidades existentes en los sistemas de información de la organización de acuerdo a los requisitos de seguridad de la información establecidos en la política.
Alcance	Cualquier organización
Referencia ISO 27001	A.18.2.3
Guía de implementación	Se deben identificar los sistemas críticos a ser revisados periódicamente y se debe contar con procedimientos formales para la realización de las revisiones. Se debe definir al responsable de la gestión de las revisiones periódicas. Los procedimientos de revisión se deben incorporar al SGSI y deben actualizarse ante cualquier cambio que lo amerite. Se deben realizar como mínimo pruebas de intrusión (ethical hacking) y evaluaciones de vulnerabilidades. Las mismas pueden llevarse a cabo con recursos propios de la organización o con apoyo externo. Asimismo, deben confeccionarse informes y comunicar los resultados y planes de acción para las correcciones a las áreas funcionales necesarias, así como a la Dirección.
Administración Central	-

Instituciones de salud	Se debe considerar la revisión regular de los sistemas que sean críticos para la atención clínica (por ejemplo, HCE, LIS, RIS, PACS, equipos biomédicos, entre otros) y aquellos que afecten o puedan afectar a la infraestructura de HCEN o sus sistemas circundantes.
Guía de evidencia para auditoría	• Evidencia de la realización de pruebas de intrusión. • Plan de acción para las acciones correctivas.
Normativa asociada	N/A
Documentación de apoyo asociada	N/A
Requisito CN.4	Gestionar las licencias de software.
Objetivo	Mantener el número óptimo de licencias para soportar de forma adecuada los requerimientos de las operaciones y documentar su uso.
Alcance	Cualquier organización
Referencia ISO 27001	A.8.1.1, A.8.1.2, A.18.1.2
Guía de implementación	Se debe mantener al día la documentación que acredite la propiedad de las licencias de software, así como cumplir con sus términos y condiciones de uso. Se debe contar con información que indique en qué momento se adquirieron las licencias, si están asociadas a un contrato y en uso. En ese caso, también se debe contar con información que indique cuántas son y en dónde se encuentran instaladas, su costo, etc.
Administración Central	-
Instituciones de salud	-
Guía de evidencia para auditoría	• Documentación asociada al licenciamiento. • Evidencia de las revisiones de licenciamiento realizadas en el período auditado. • Inventario de equipamiento y detalle de software instalado. • Para cada software instalado, detalle del servidor, indicar si se utiliza virtualización, detalle de la contingencia (hot, warm, etc.), entre otros.
Normativa asociada	N/A
Documentación de apoyo asociada	N/A

5 Glosario

5.1 Abreviaturas

DNS	Domain Name System (Sistema de Nombres de Dominio)
CAdES CMS	Advanced Electronic Signatures is a set of extensions to Cryptographic Message Syntax (CMS) signed data making it suitable for advanced electronic signatures.
CCTV	Closed Circuit Television (Circuito Cerrado de Televisión)
CDA	Clinical Document Architecture (Arquitectura de Documento Clínico)
CERTuy	Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay
CSI	Comité de Seguridad de la Información
CSIRT	Computer Security Incident Response Team (Equipo de Respuesta ante Incidentes de Seguridad Informática)
HCE	Historia Clínica Electrónica
HCEN	Historia Clínica Electrónica Nacional
HIS	Hospital Information System (Sistema de Información Hospitalaria)
HTTPS	Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
HSM	Hardware Security Module (Módulo de Seguridad Hardware)
ICMP	Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
IP	Internet Protocol (Protocolo IP)
IPS	Intrusion Prevention System (Sistema de Prevención de Intrusos)
LAN	Local Area Network (Red de Área Local)
LIS	Laboratory Information System (Sistema de Información de Laboratorio)
MUA	Mail User Agent (Agente de Usuario de Correo)
MTA	Mail Transfer Agent (Agente de Transferencia de Correo)
PACS	Picture Archiving and Communication System (Sistema de Archivo y Transmisión de Imágenes)
PGP	Pretty Good Privacy (Privacidad Bastante Buena)

RSI	Responsable de la Seguridad de la Información
SAN	Storage Area Network (Red de Área de Almacenamiento)
SI	Seguridad de la Información
SGSI	Sistema de Gestión de Seguridad de la Información
SLA	Service Level Agreement (Acuerdo de Nivel de Servicio)
SNMP	Simple Network Management Protocol (Protocolo Simple de Administración de Red)
SO	Sistema Operativo
SSL	Secure Sockets Layer (Capa de Puertos Seguros)
TCP/IP	Transmission Control Protocol and the Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet)
TI	Tecnología de la Información
TIC	Tecnología de la Información y la Comunicación
TLS	Transport Layer Security (Seguridad de la Capa de Transporte)
UCE	Unidad de Certificación Electrónica
UE	Unidad Ejecutora
RTO	Recovery Time Objective (Tiempo de Recuperación Objetivo)
RPO	Recovery Point Objective (Punto de Recuperación Objetivo)
URCDP	Unidad Reguladora y de Control de Datos Personales
VPN	Virtual Private Network (Red Privada Virtual)
WAF	Web Application Firewall
WIFI	Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica
WRT	Work Recovery Time (Tiempo de Recuperación de Trabajo)
XADES	XML Advanced Electronic Signatures (Firma electrónica avanzada XML)
XDS	Cross-Enterprise Document Sharing (Intercambio de Documentos entre Empresas)
XML	Extensible Markup Language (Lenguaje de Marcado Extensible)

5.2 Definiciones

A

Activos de información

Son aquellos datos o información que tienen valor para el organismo. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones].

Activos de información críticos del Estado

Son aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía del país. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

Antivirus
Sistemas informáticos cuyo objetivo es detectar o eliminar virus informáticos.

Antispyware
Sistema informático que permite detectar o eliminar spyware (programas espías) que transmiten información a una entidad externa sin el conocimiento o consentimiento del usuario.

Áreas seguras o protegidas

Áreas donde se procesa y almacena la información y/o respaldos; por ejemplo, centro de datos y archivos.

Acceso privilegiado

Cuando se requiere acceso a funciones de administración de usuarios, roles, grupos y perfiles (creación, modificación, bloqueo e inactivación de cuentas de usuario) y/o parametrización (cambios a los parámetros de configuración, tablas básicas, archivos de configuración).

C

CAdES CMS Advanced Electronic Signatures

Conjunto de extensiones a los datos firmados con CMS Cryptographic Message Syntax (Sintáxis de Mensajes Criptográficos) que lo hacen adecuado para firmas electrónicas avanzadas.

CCTV Closed Circuit Television (Circuito Cerrado de Televisión).

Tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades.

CDA Clinical Document Architecture (Arquitectura de Documento Clínico).

Documento intercambiable en los procesos de interoperabilidad. Corresponde a los actos clínicos o eventos en salud que se registran en la institución prestadora de los servicios de salud, y que pueden ser compartidos o intercambiados acorde con la dinámica establecida y a las políticas de seguridad de la información del marco jurídico.

CERTuy Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay.
El CERTuy protege los activos de información críticos del Estado y promueve el conocimiento en seguridad de la información de manera de prevenir y responder a incidentes de seguridad

Control
Medio de gestionar el riesgo, incluyendo políticas, procedimientos, guías, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, de gestión, o legal. [UNIT-ISO/IEC 27000:2013]

D

DNS Domain Name System (Sistema de Nombres de Dominio)
Sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

E

Evento de seguridad informática
Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

Ethical hacking (hackeo ético)
Utilización de técnicas de ataque para encontrar fallas de seguridad, realizas con el permiso de la organización, con el fin de mejorar la seguridad.

F

Factor de doble autenticación
Medida de seguridad que frecuentemente requiere de un código obtenido a partir por ejemplo de una aplicación, un dispositivo o un mensaje SMS, además de una contraseña para acceder al servicio.

H

HASH
Algoritmo que, a partir de una entrada (texto, archivo, etc.) crea una salida alfanumérica que representa un resumen de toda la información de entrada y que solo puede crearse nuevamente con la misma información.

HCE Historia Clínica Electrónica
Es el conjunto integral de datos clínicos, sociales y económicos, referidos a la salud de una persona, desde su nacimiento hasta su muerte, procesados a través de medios electrónicos, siendo el equivalente funcional de la historia clínica papel.

HCEN Historia Clínica Electrónica Nacional
Plataforma de Historia Clínica Electrónica Nacional. Es la infraestructura tecnológica y de servicios que permite la conectividad de los diferentes sistemas de información del conjunto de Instituciones con competencias legales en materia de salud, públicas y privadas, con el objetivo de intercambiar información clínica.

HIS Hospital Information System (Sistema de Información Hospitalaria)
Sistema de Información Hospitalaria, también conocido como sistema de información en salud. Este sistema apoya a las instituciones de salud en la gestión de las actividades operativas, tácticas y estratégicas.

HSM Hardware Security Module (Módulo de Seguridad Hardware)
Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

HTTPS Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
Protocolo de aplicación basado en el protocolo HTTP (Hyper Text Transfer Protocol), destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

I

ICMP Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
Es un subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Es utilizado para enviar mensajes de error, indicando por ejemplo que un enrutador o host no puede ser localizado.

Incidente de seguridad de la información
Un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información. [ISO/IEC 27035:2011]

Incidente de seguridad informática
Es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). [Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

Información sensible
Información personal privada de un individuo tales como contraseñas, información personal

que revele origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

IP Internet Protocol (Protocolo de Internet)
Número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión)
de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo IP, que corresponde al nivel de red del modelo TCP/IP.

IPS Intrusion Prevention System (Sistema de Prevención de Intrusos)
Software que ejerce el control de acceso en una red informática para proteger a los sistemas ante ataques y abusos.

L

LIS Laboratory Information System (Sistema de Información de Laboratorio)
También conocido como LIMS Laboratory Information Management System (Sistema de Gestión de Información de Laboratorio). Es un sistema que soporta por ejemplo la gestión del flujo de trabajo en laboratorios de análisis clínicos desde el seguimiento de muestras hasta múltiples aspectos de la informática de laboratorios.

LOG Historial de log o registro
Registro de todos los acontecimientos, eventos o acciones que afectan un proceso informático en particular y constituye una evidencia del comportamiento del sistema.

M

MTD Maximum Tolerable Downtime (Tiempo de inactividad máximo tolerable).
Se trata de la cantidad máxima de tiempo que una organización puede estar sin operar sin causar daños irreparables al negocio.
MTD = RTO + WRT

mod_security
Es un módulo del servidor Web Apache que provee protección contra diversos ataques hacia aplicaciones Web y permite monitorizar tráfico HTTP, así como realizar análisis en tiempo real sin necesidad de hacer cambios a la infraestructura existente.

P

PACS Picture Archiving and Communication System (Sistema de Archivo y Transmisión de Imágenes)
Sistema computarizado para el archivo digital de imágenes médicas.

Personal
En el ámbito de la administración central, hace referencia a personal presupuestado, contratado, pasantes, no incluye proveedores de servicio.

PGP Pretty Good Privacy (Privacidad Bastante Buena)
Programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información

distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

R

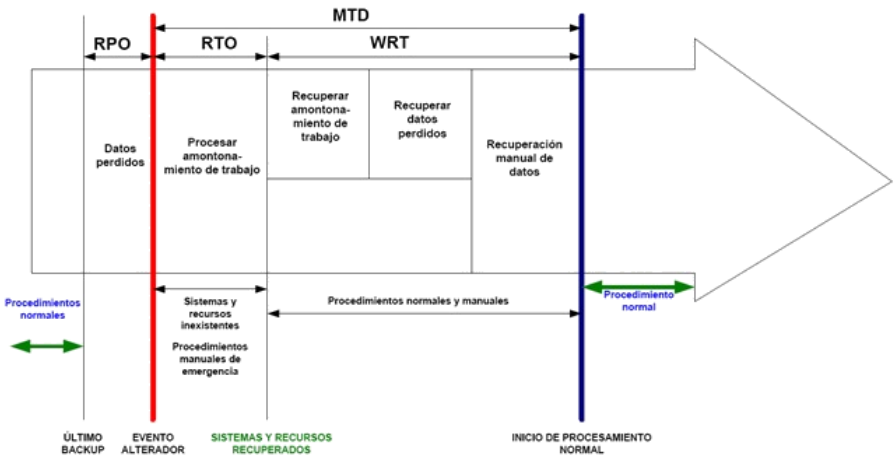
Red Salud
Es una red privada para la conexión de Instituciones con competencias legales en la materia de salud, públicas y privadas, a través de la Plataforma de Historia Clínica Electrónica Nacional, que permite el intercambio seguro de información de los usuarios del sistema de salud.

RIS Radiology Information System (Sistema de Información de Radiología)
Sistema para la gestión y el control del diagnóstico por imagen (por ejemplo, turnos, insumos, facturación, informes de diagnóstico, estadísticas). Habitualmente conectado a los sistemas HIS y PACS.

Router (Enrutador)
Dispositivo que proporciona conectividad a nivel de capa 3 o capa de red del modelo OSI Open System Interconection (Sistema Abierto de Interconexión).

RPO Recovery Point Objective (Punto de Recuperación Objetivo)
La máxima cantidad de información que se puede perder de acuerdo al cronograma de realización de copias de respaldo y/o necesidades de información que se presenten. En otras palabras, indica el tiempo máximo que una organización acepta respecto a pérdida de datos desde el último respaldo. Por ejemplo, las transacciones de hasta cuánto tiempo atrás se está dispuesto a perder o reintroducir al sistema.

RTO Recovery Time Objective (Tiempo de Recuperación Objetivo)
Tiempo requerido para que los sistemas críticos de la Organización estén nuevamente operando. En otras palabras, indica la cantidad de tiempo en que se puede realmente recuperar los procesos en caso de disrupción.
Se busca siempre que los tiempos de los RTOs sean menores que los de los MTDs.



S

Sistema informático
Los ordenadores y redes de comunicación electrónica, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. [Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

Smart Card (Tarjeta inteligente)
Tarjeta inteligente con circuitos integrados, que permite la ejecución de cierta lógica programada.

SNMP Simple Network Management Protocol (Protocolo Simple de Administración de Red)
Protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

Switch (Conmutador)
Dispositivo digital lógico de interconexión de equipos que opera a nivel de capa 2 o capa de enlace de datos (del modelo OSI).

T

TCP/IP Transmission Control Protocol (TCP) and the Internet Protocol (IP) (Protocolo de control de transmisión/Protocolo de Internet)
Descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970.

TLS Transport Layer Security (Seguridad de la Capa de Transporte)
Protocolo criptográfico que proporciona comunicaciones seguras por una red.

Token
Dispositivo electrónico que se le da a un usuario autorizado de un servicio informático para facilitar el proceso de autenticación.

U

UCE Unidad de Certificación Electrónica
Creada por el artículo 12 de la Ley N° 18.600 de Documento Electrónico y Firma Electrónica, como un órgano desconcentrado de Agesic. Sus cometidos y funciones son: acreditación, control, instrucción, regulación y sanción.

URCDP Unidad Reguladora y de Control de Datos Personales
Unidad creada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP), con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios.

Usuario privilegiado
Usuario que requiere acceso privilegiado para realizar funciones específicas.

V

VPN Virtual Private Network (Red Privada Virtual)
Tecnología de red de computadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

W

Webmail
Un Webmail o correo Web es un cliente de correo electrónico, que provee una interfaz Web por la que accede al correo electrónico.

WRT Work Recovery Time (Tiempo de Recuperación de Trabajo)
Tiempo requerido para recuperar la información perdida (Basado en el RPO), así como de ingresar al sistema todos los datos que se generaron durante la caída del sistema.

X

XADES XML Advanced Electronic Signatures (Firma electrónica avanzada XML)
Es un conjunto de extensiones a las recomendaciones XML-DSig (Firma XML; recomendación del W3C World Wide Web Consortium que define una sintaxis XML para la firma digital haciéndolas adecuadas para la firma electrónica avanzada).

XDS Cross-Enterprise Document Sharing (Intercambio de Documentos entre Empresas)
Especificación basada en estándares para administrar el intercambio de documentos entre cualquier empresa de atención médica, desde un consultorio médico privado hasta una clínica, un centro de cuidados intensivos para pacientes internados y sistemas de registros de salud personales.

XML Extensible Markup Language (Lenguaje de Marcado Extensible)
Meta-lenguaje que permite definir lenguajes de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible.

X.509 v3
Estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. La última versión es la 3, de mayo de 2008.