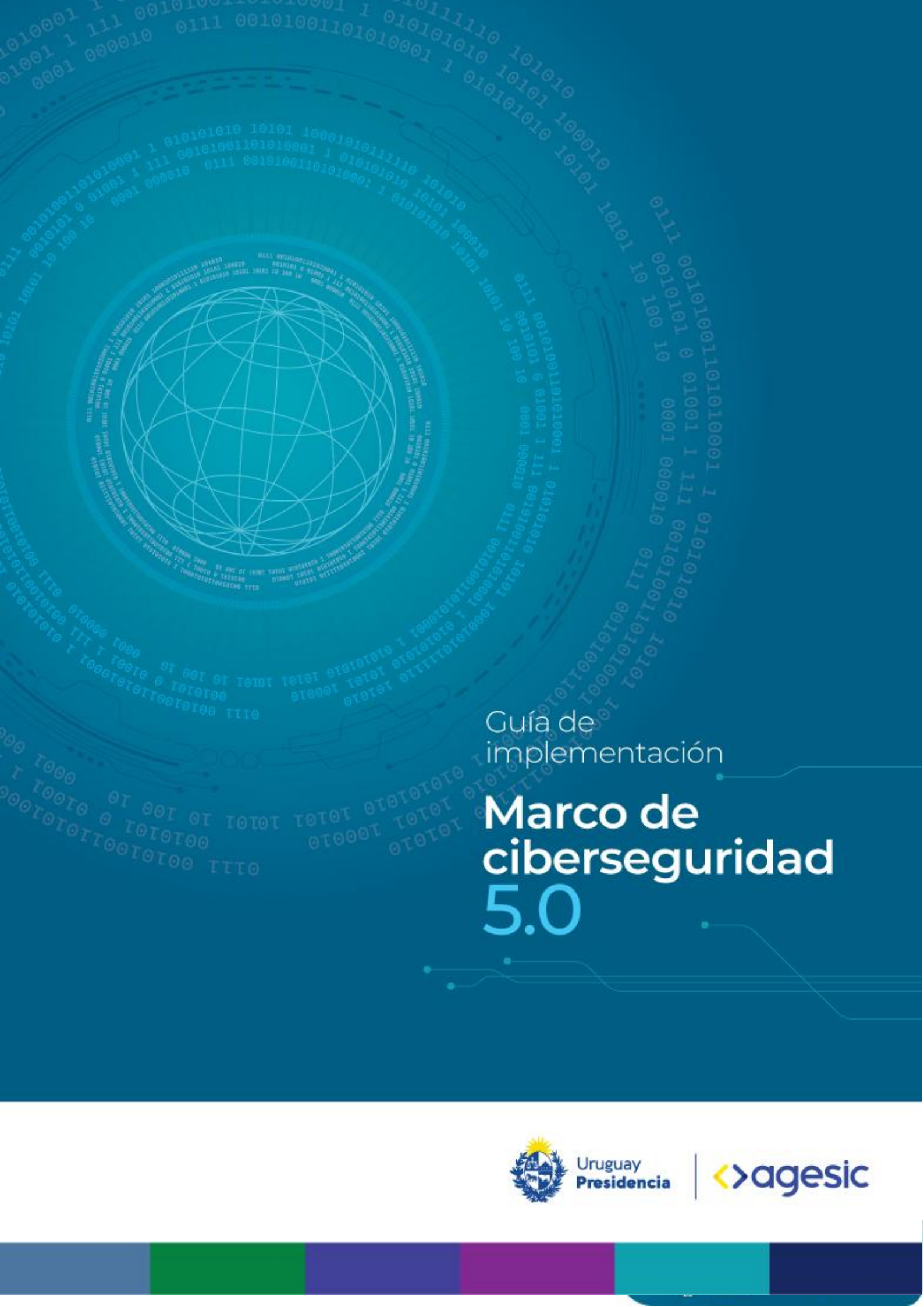

Guía de implementación

Marco de ciberseguridad 5.0

Uruguay Presidencia | agesic

SEGURIDAD DE LA INFORMACIÓN

Versión 5.0 – Agosto 2025

Introducción

Los requisitos de esta Guía se encuentran asociados a las subcategorías del Marco de Ciberseguridad.

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.

1. Objetivo y alcance

Los objetivos específicos son:

- Establecer los requisitos que se entienden necesarios para implantar una adecuada gestión de la seguridad de la información y ciberseguridad.
- Explicar el objetivo de cada uno de los requisitos.
- Brindar una guía de implementación basada en las mejores prácticas internacionales.
- Proveer documentación de apoyo que pueda ser reutilizada y adaptada por cada organización, entre otras guías y recursos, para implementar los requisitos.

2. 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.
Controles	Descripción de controles mínimos para dar cumplimiento al requisito, ordenados por nivel de madurez.
Guía de implementación	Sugerencias, mejores prácticas y/o guías metodológicas para lograr alcanzar el objetivo y, por consiguiente, implementar el requisito.
Instituciones de salud	Aspectos específicos aplicables a la realidad de las instituciones de salud.
Instituciones Emisoras de Dinero Electrónico (IEDE)	Aspectos específicos aplicables a la realidad de las Instituciones Emisoras de Dinero Electrónico.
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 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.

2.1 Organización y Gobernanza

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.
Controles	Nivel 1: PS.1-1: Existe una política de seguridad aprobada por la Dirección. PS.1-2: La política es difundida a todo el personal y partes interesadas relevantes. Nivel 2: PS.1-3: La política define los responsables de su cumplimiento. PS.1-4: La política se encuentra disponible en un sitio accesible.

	Nivel 3: PS.1-5: La política es revisada ante cambios significativos de índole normativo o del contexto de la organización. PS.1-6: Los resultados de las revisiones de la política son documentados y comunicado al CSI. PS.1-7: Ante modificaciones la política es difundida nuevamente. Nivel 4: PS.1-8: La política es revisada periódicamente. PS.1-9: La política cuenta con indicadores definidos para su evaluación.
Guía de implementación	**Política de Seguridad de la Información** 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. **Aprobación y difusión** 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. **Revisión** 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.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	● Resolución con la adopción de la Política de Seguridad de la Información, u otro mecanismo o registros que evidencie la Política formalmente aprobada. ● Acceso a la publicación de la Política de Seguridad de la Información (por ejemplo, sitio institucional, Intranet, otros) y evidencia de su difusión. ● Cuestionarios al personal para corroborar el conocimiento de la Política de Seguridad de la Información. ● Registro 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	-

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.
Controles	Nivel 1: OR.1-1: Existe una persona que cumple el rol de RSI. OR.1-2: El RSI coordina actividades de seguridad de la información. Nivel 2: OR.1-3: Está designado formalmente el RSI. OR.1-4: Las responsabilidades del RSI están documentadas e incluyen: la gestión de seguridad de la información, gestión de incidentes, gestión de riesgos de seguridad, entre otras. Nivel 3: OR.1-5: El RSI coordina la evaluación de riesgos de seguridad de la información junto con los responsables de los activos o designa referentes delegados. OR.1-6: El RSI participa en el CSI de la organización. Nivel 4: OR.1-7: El RSI elabora y presenta planes anuales de mejora de seguridad de la información, incluyendo indicadores. OR.1-8: El RSI forma parte de los procesos de planificación estratégica.
Guía de implementación	**Responsable de la Seguridad de la Información (RSI)** La organización debe designar a un RSI de la Información que, idealmente, 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 que podrá ser interna o externa, debe contar con disponibilidad para cumplir adecuadamente con las funciones asignadas; debe contar con los mecanismos para contactar 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 RSI. Se entiende necesario determinar la dedicación que debe tener quien asuma el rol en la organización. **Cometidos** El RSI o quien éste determine, debe ser el punto de contacto con el CERTuy.

	Reunir y responder información que el CERTuy solicite a la entidad, para un entendimiento cabal de los sistemas relacionados con TIC necesaria para la adecuada resolución de los incidentes de ciberseguridad, en los tiempos que éste determine. Participar, con las autoridades competentes en la entidad, en los casos que el CERTuy entienda necesario, de proyectos con el fin de facilitar el monitoreo de los sistemas informáticos, con el fin de prevenir posibles incidentes de ciberseguridad, de acuerdo con el CERTuy o la autoridad sectorial competente. Cumplir las condiciones, requisitos e informaciones mínimas que debe proveer la entidad, para comunicar los incidentes de ciberseguridad, de acuerdo con lineamientos del CERTuy o la autoridad sectorial competente. Notificar cuando existen cambios sustantivos en los sistemas y cuando se incorporan nuevos. Proporcionar información de los sistemas existentes, así como información de cómo funciona el sistema para poder interpretar las trazas de auditoría de los mismos.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Resolución de designación del rol del RSI u otro mecanismo o registros que evidencie formalmente la designación. • Difusión de la designación del rol de RSI (correo, sitio web, intranet, etc.). • Descripción de cargo o rol de RSI. • Notificación de designación a AGESIC (correo, etc.). • Actas o evidencias de reuniones del CSI donde participe el RSI. • Organigrama donde figure el RSI. • Planes de mejora firmados o aprobados por el RSI. • Evidencia de participación del RSI en evaluación de riesgos.
Normativa asociada	Ley 20.212, art. 78 Decreto 66/025, art. 8,10, 11 Compromiso de uso adecuado de la Red Salud.

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.
Controles	Nivel 1: OR.2-1: Se encuentra designado formalmente el CSI de la organización. Nivel 2: OR.2-2: El CSI se reúne periódicamente y documenta dichas reuniones. Nivel 3: OR.2-3: Las responsabilidades y atribuciones del CSI están documentadas y aprobadas por la Dirección. OR.2-4: El CSI tiene establecidas pautas para su funcionamiento. OR.2-5: El CSI participa en la definición de niveles aceptables de riesgo y en la aprobación del plan de tratamiento de riesgos. Nivel 4: OR.2-6: El CSI revisa los planes y políticas de seguridad y aprueba sus actualizaciones. OR.2-7: El CSI aprueba la planificación estratégica de seguridad. OR.2-8: El CSI revisa los indicadores asociados a los planes anuales de mejora de seguridad de la información.
Guía de implementación	**Comité de Seguridad de la Información** 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. Dependiendo de la realidad y tamaño de la organización, los cometidos del CSI podrían incluirse a otros grupos ya existentes como por ejemplo el "Gabinete ministerial" o la reunión "Gerencial". **Conformación** En términos generales, su conformación refiere a directivos con toma de decisiones dentro de la organización. Si la organización 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. Esta situación también podría darse en otros escenarios, por ejemplo, en el ámbito privado con casa matriz y sucursales. **Funcionamiento** 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. **Cometidos** 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.
Instituciones de salud	Además de lo planteado en términos generales, el CSI debe contar con al menos un miembro perteneciente al área asistencial.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Resolución de la creación del CSI, u otro mecanismo o registros que evidencie su creación. • Responsabilidades del CSI aprobados por la Dirección. • Pautas de funcionamiento del CSI. • Registro de las reuniones mantenidas por el CSI durante el período auditado (actas, orden del día, correos, otros). • Registro de evaluaciones del funcionamiento del CSI. • Registro de aprobaciones de políticas y modificaciones de políticas por el CSI (minutas, actas, correos, formularios, otros). • Plan de tratamiento de riesgos aprobado por el CSI.
Normativa asociada	N/A

Requisito OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.
Objetivo	Contribuir con las buenas prácticas de gestión dentro de la organización definiendo un procedimiento documentado de contacto con autoridades (internas y externas), vinculadas a regulación y cumplimiento en materia de seguridad de la información y ciberseguridad, particularmente, las que deban ser contactadas antes un incidente de ciberseguridad.
Controles	Nivel 1: OR.3-1: Está designado un punto de contacto oficial para incidentes de ciberseguridad. OR.3-2: Se han identificado los contactos de autoridades ante aspectos de ciberseguridad. Nivel 2: OR.3-3: El punto de contacto oficial es conocido por todo el personal. Nivel 3:

	OR.3-4: Los contactos con las autoridades, CSIRT y otros actores externos relevantes están documentados. Nivel 4: OR.3-5: Se revisan y actualizan periódicamente los contactos.
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 autoridades y equipos 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. Dicho procedimiento debe definir específicamente cómo, y ante que casos, contactar al CERTuy (responsables, canales de comunicación, difusión del procedimiento) así como con URCDP, el Ministerio del Interior u otras autoridades; este procedimiento deberá basarse en las guías y normativa asociada vigente. 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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	Los incidentes deben ser comunicados al BCU conforme normativa vigente.
Guía de evidencia para auditoría	• Comunicación formal con autoridades (correo, expediente, nota, etc.) • Lista de contactos • Designación del contacto ante para incidentes de ciberseguridad.
Normativa asociada	Ley 20.212, art. 78 Decreto 66/025, art. 8 literial i, 10, 11

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 y ciberseguridad estén incluidos en todos los proyectos desde su inicio.
Controles	Nivel 1: OR.4-1: Se tiene una lista actualizada de proyectos (finalizados, en curso o planificados) de la organización. Nivel 2: OR.4-2: Se incluye al RSI o a quien éste designe en la etapa de planificación o inicio de los proyectos. OR.4-3: Los contratos y pliegos vinculados a los proyectos contemplan cláusulas de seguridad. Nivel 3: OR.4-4: La documentación de los proyectos incluye requisitos de seguridad de la información. OR.4-5: La evaluación de riesgos del proyecto incluye riesgos de seguridad de la información. OR.4-6: Los informes de avance del proyecto deben incluir el seguimiento del tratamiento de los riesgos de seguridad. Nivel 4: OR.4-7: Se evalúa el cumplimiento de los requisitos de seguridad al finalizar un proyecto. OR.4-8: Se documentan las lecciones aprendidas sobre seguridad para la gestión de proyectos futuros.
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. Se gestiona la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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.

	• Registros 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. • Actas de cierre con evaluación de cumplimiento de requisitos de seguridad. • Contratos y pliegos de los proyectos. • Documento de lecciones aprendidas del proyecto.
Normativa 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.
Controles	Nivel 1: OR.5-1: Se mantiene un inventario actualizado de los dispositivos móviles de la organización. OR.5-2: Estos activos cuentan con al menos un factor de autenticación para acceder a la información. OR.5-3: Existen pautas que regulan el uso de los dispositivos móviles. Nivel 2: OR.5-4: Las pautas de uso son comunicadas al personal y partes interesadas. OR.5-5: Los dispositivos de la organización cumplen con requisitos de seguridad como: antimalware, cifrado de disco, bloqueo, versión mínima de sistema operativo. Nivel 3: OR.5-6: Los equipos móviles cuentan con un sistema de borrado del dispositivo en caso de extravío o robo. OR.5-7: Los dispositivos personales que se conectan a los servicios de la organización deben estar autorizados, registrados y sujetos a requisitos de seguridad. OR.5-8: Existe una política formalmente aprobada de uso aceptable de dispositivos móviles. Nivel 4: OR.5-9: Se revisa y actualiza la política de uso de los dispositivos móviles periódicamente o ante cambios tecnológicos o normativos. OR.5-10: Se revisan y actualizan los procedimientos asociados al correcto uso de los dispositivos móviles.
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.
Instituciones de salud	**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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. ● Registros de revisión periódica de la política (minutas, actas, correos, formularios, otros). ● Registro de difusión de la política de uso de dispositivos móviles.
Normativa asociada	N/A

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.
Controles	Nivel 1: OR.6-1: Están definidos requisitos de seguridad mínimos para los dispositivos que se utilicen para acceder remotamente a los activos de la organización. Nivel 2: OR.6-2: Se registra cada conexión remota como mínimo: hora, fecha, usuario, activo, etc. OR.6-3: Se otorga el acceso remoto con base en una lista blanca de todos los recursos disponibles. OR.6-4: Se implementa el múltiple factor de autenticación para el acceso remoto. OR.6-5: Se requiere la aprobación explícita del responsable del activo antes de habilitar el acceso remoto.

	Nivel 3: OR.6-6: Existe un procedimiento documentado de solicitud de acceso remoto. OR.6-7: Existe un responsable para la asignación de permisos de acceso remoto. OR.6-8: Esta definida una política de control de acceso remoto. OR.6-9: Los proveedores tienen permisos de acceso remoto que caducan luego de realizada la actividad (o de una fecha establecida) para la cual se les otorgó el acceso. OR.6-10: Al menos en forma administrativa se centraliza el acceso remoto. Nivel 4: OR.6-11: Se realizan revisiones periódicas de los usuarios con acceso remoto. OR.6-12: El resultado de las revisiones retroalimenta la gestión del acceso remoto y proporciona información para la toma de decisiones de mejora continua. OR.6-13: Se realizan actividades de control interno para verificar el cumplimiento de los procedimientos establecidos.
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** Los mecanismos de autenticación seguros son los métodos y procesos que se utilizan para verificar la identidad de un usuario, dispositivo o sistema de una manera fiable y resistente a los ataques. El objetivo principal es garantizar que solo las entidades autorizadas puedan acceder a datos, sistemas o recursos protegidos. Por ejemplo: múltiples factores de autenticación, contraseña de un solo uso, autenticación biométrica, entre otros. 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 deben 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. **Mecanismos de seguridad para el acceso remoto** Se deberán utilizar mecanismos seguros para el acceso remoto, cómo por ejemplo MFA, que garanticen la privacidad, confidencialidad e integridad de la información. El acceso remoto debe 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.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Registros de revisiones de acceso remoto. • Registros de conexión remota.
Normativa asociada	

Requisito OR.7	Conocer el contexto de la organización
Objetivo	Conocer e identificar las partes interesadas y servicios que son críticos para el correcto funcionamiento de la organización y los servicios que brinda.
Controles	Nivel 1: OR.7-1: Se han identificado los servicios críticos para la organización.

	OR.7-2: Se han identificado los proveedores y/o otras partes interesadas críticas para la organización. Nivel 2: OR.7-3: Se cuenta con un mapeo de procesos. OR.7-4: Se realiza un análisis del contexto interno y externo (por ej, análisis FODA u otro equivalente), considerando factores relevantes que puedan impactar en la seguridad de la información. Nivel 3: OR.7-5: Se cuenta con un mapeo de dependencias entre servicios, procesos y proveedores críticos. Nivel 4: OR.7-6: Se realizan revisiones periódicas y sistemáticas del contexto de la organización, considerando cambios internos, externos, regulatorios y tecnológicos.
Guía de implementación	**Identificación de servicios críticos y partes interesadas** La organización debe identificar y documentar los servicios críticos necesarios para el cumplimiento de sus objetivos estratégicos y operativos. Asimismo, se deben identificar y registrar los proveedores y demás partes interesadas críticas que impactan directa o indirectamente en dichos servicios. Esta información debe mantenerse actualizada y disponible para la gestión de riesgos y la planificación de la continuidad de negocio. **Mapeo de procesos y análisis de contexto** Se debe contar con un mapeo documentado de los procesos organizacionales que permita visualizar las principales actividades, sus responsables y la relación con los servicios críticos. A su vez, la organización debe realizar un análisis del contexto interno y externo que incluya factores políticos, económicos, sociales, tecnológicos, legales y ambientales que puedan afectar a la seguridad de la información. Herramientas como el análisis FODA, o metodologías equivalentes, pueden ser utilizadas para este fin. **Mapeo de dependencias** Es necesario identificar y documentar las dependencias entre servicios, procesos y proveedores críticos, con el objetivo de reconocer posibles puntos únicos de falla que puedan comprometer la operación de la organización. Este mapeo debe ser utilizado como insumo para el análisis de riesgos y para el diseño de estrategias de resiliencia. **Revisión periódica y actualización** La organización debe realizar revisiones periódicas y sistemáticas de su contexto, considerando tanto cambios internos (procesos, estructura, servicios) como externos (regulatorios, tecnológicos, de mercado o de seguridad). Estas revisiones deben documentarse y reflejarse en la actualización de los mapeos, análisis y dependencias, asegurando que la información se mantenga vigente y relevante para la toma de decisiones.

Instituciones de salud	
Instituciones Emisoras de Dinero Electrónico (IEDE)	
Guía de evidencia para auditoría	• Documentación que identifique los servicios críticos de la organización (listados, informes, planes estratégicos u operativos). • Registro actualizado de proveedores y partes interesadas críticas. • Informe de análisis del contexto interno y externo (por ejemplo, FODA, PESTEL o equivalente), con fecha de elaboración y responsables. • Documentación del mapeo de dependencias entre procesos, servicios y proveedores, incluyendo identificación de posibles puntos únicos de falla.
Normativa asociada	

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.
Controles	Nivel 1: PL.1-1: Están establecidos los objetivos anuales de seguridad de la información. PL.1-2: Están definidas las acciones para lograr el cumplimiento de los objetivos. Nivel 2: PL.1-3: Los objetivos forman parte de un plan de acción de seguridad de la información. PL.1-4: Los objetivos están documentados y aprobados por el CSI. Nivel 3: PL.1-5: Los objetivos anuales de seguridad de la información son difundidos al personal y partes interesadas. PL.1-6: El plan de acción para cumplir con los objetivos se desarrolla y ejecuta de manera coordinada con los distintos actores de la organización. PL.1-7: Se definen indicadores para el seguimiento del cumplimiento de los objetivos. Nivel 4: PL.1-8: Los objetivos se traducen en proyectos o iniciativas de seguridad de la información. PL.1-9: Se revisa periódicamente el cumplimiento de los objetivos y el avance del plan de acción.
Guía de implementación	**Estrategia y objetivos** Se debe 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 deben derivar proyectos concretos de seguridad de la información. Se pueden establecer indicadores para el seguimiento del cumplimiento de los objetivos planteados.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Indicadores de seguimiento.
Normativa asociada	N/A

2.2 Gestión de riesgos

Requisito GR.1	Adoptar una metodología de Evaluación de Riesgo.
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 de riesgo, la tolerancia sobre las desviaciones, calcular la probabilidad de ocurrencia y el impacto potencial sobre la materialización de las vulnerabilidades.
Controles	Nivel 1: GR.1-1: Existe un proceso para la gestión de riesgos de seguridad de la información que abarca los componentes del centro de procesamiento de datos y servicios críticos de forma independiente. Nivel 2: GR.1-2: Se cuenta con una metodología de evaluación de riesgos de seguridad de la información definida y documentada. Nivel 3:

	GR.1-3: Existe una política aprobada de gestión de riesgos de seguridad de la información. GR.1-4: La política de gestión de riesgos de seguridad de la información ha sido difundida a todas las partes interesadas. Nivel 4: GR.1-5: La metodología de evaluación de riesgos es revisada periódicamente y ajustada en función de los resultados obtenidos, los cambios en el contexto organizacional o normativo, y las oportunidades de mejora identificadas en su aplicación.
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. Dentro de los riesgos a identificar, deberán incluirse los riesgos positivos (es decir, las oportunidades estratégicas); de manera de permitir la discusión de estos aspectos en las evaluaciones de riesgos de ciberseguridad. **Política** 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. **Aprobación y difusión** La política de gestión 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 y/o CSI.
Instituciones de salud	
Instituciones Emisoras de Dinero Electrónico (IEDE)	El órgano de dirección de la institución definirá, aprobará y supervisará todas las disposiciones relacionadas con el marco de gestión del riesgo. Los líderes de la organización son responsables de los riesgos de ciberseguridad y fomentan una cultura consciente de los riesgos, manteniendo una mejora continua en los procesos de gestión de riesgos. La institución cuenta con un seguro que cubre costos asociados a ciberataques.
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. ● Cuestionarios realizados al personal para corroborar el conocimiento de la Política de gestión de riesgo. ● Registro de cambios a la Política de gestión de riesgo.
Normativa asociada	N/A

Requisito GR.2	Realizar de manera sistemática el proceso de evaluación de riesgos.
Objetivo	Contribuir al cumplimiento de los objetivos de seguridad de la información, prevenir o reducir los efectos no deseados y lograr la mejora continua.
Controles	Nivel 1: GR.2-1: Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia. Nivel 2: GR.2-2: Las amenazas, vulnerabilidades y controles existentes en la organización están documentados. GR.2-3: Se cuenta con un inventario de riesgos de seguridad de la información que incluye riesgos asociados a todos los activos de información (se incluyen riesgos positivos). Nivel 3: GR.2-4: El apetito de riesgo y la tolerancia al riesgo se ha definido formalmente por el negocio. GR.2-5: Se incorporan riesgos vinculados a la cadena de suministro. GR.2-6: Los incidentes de seguridad de la información y ciberseguridad son tenidos en cuenta para la evaluación de riesgos. Nivel 4: GR.2-7: Debe revisarse periódicamente la tolerancia al riesgo establecida, y modificarse ante cambios normativos, tecnológicos o necesidades del negocio. GR.2-8: Los riesgos se revisan periódicamente, la revisión se documenta formalmente.
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. • Clasificar y monitorear los riesgos. • Establecer la periodicidad de las evaluaciones. Los riesgos deben ser evaluados en toda la cadena de suministro y delegar obligaciones en los casos que corresponda.
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.

Instituciones Emisoras de Dinero Electrónico (IEDE)	Se gestionan los riesgos de las API o Servicios Web suministrados por los proveedores de servicios de computación en la nube.
Guía de evidencia para auditoría	• Inventario de riesgos identificados y seguimiento para el período auditado. • Evaluación y/o análisis de riesgos. • Evaluaciones de riesgos de proveedores críticos.
Normativa asociada	N/A

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 tratar (aceptar, eliminar, mitigar o transferir) 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.
Controles	Nivel 1: GR.3-1: Se toman acciones ad-hoc con el objetivo de llevar los principales riesgos de seguridad de la información a niveles aceptables para la organización. Nivel 2: GR.3-2: Se elaboran planes de tratamiento para los riesgos de seguridad de la información que excedan los niveles de tolerancia definidos por la organización. GR.3-3: Cada plan de tratamiento identifica las acciones necesarias, el responsable de su ejecución y el plazo previsto. Nivel 3: GR.3-4: Los planes de tratamiento son revisados y validados por los responsables de ejecutarlos antes de su ejecución. GR.3-5: Los planes de tratamiento de riesgos incluyen métricas e indicadores que permiten evaluar su avance. GR.3-6: La implementación de los controles debe realizarse conforme a la prioridad explícita y formalmente establecida por la Dirección. GR.3-7: La efectividad de los controles implementados es evaluada, y el riesgo residual resultante es documentado y validado por las partes interesadas. GR.3-8: Existe una línea presupuestal que permite implementar el plan de tratamiento de riesgos. Nivel 4:

	GR.3-9: Los planes de tratamiento de los riesgos se revisan periódicamente y se actualizan si es necesario. GR.3-10: La revisión se documenta formalmente y es comunicada al CSI y a las otras partes interesadas.
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. ● Identificar los controles necesarios para respuesta y mitigación, además de las medidas de seguridad ya implementadas. 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. Los planes de gestión de riesgos de la cadena de suministro en materia de ciberseguridad incluyen disposiciones para las actividades que ocurren después de la conclusión de un acuerdo de colaboración o servicio.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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 reevaluación de mitigación o control de las vulnerabilidades. ● Política de gestión de riesgos. ● Inventario de riesgos de seguridad de la información. ● Matriz de riesgos (impacto, probabilidad, tolerancia, controles). ● Documentación de procesos críticos y su tolerancia al riesgo.

	• Actas o minutas de revisión de planes de tratamiento. • Reportes de indicadores de gestión de riesgos.
Normativa asociada	-

Requisito GR.4	Inteligencia de amenazas
Objetivo	La inteligencia de ciberamenazas y otra información contextual se integran en el análisis de riesgos.
Controles	Nivel 1: GR.4-1: La organización ha identificado y documentado sus fuentes confiables de inteligencia de amenazas, incluyendo al menos CERTuy y fuentes oficiales, comunitarias o sectoriales. GR.4-2: El personal de seguridad recibe capacitación sobre el uso de inteligencia de amenazas. GR.4-3: La organización recibe periódicamente información de amenazas a través de sus fuentes confiables, la misma se registra para su posterior análisis. Nivel 2: GR.4-4: Están asignados los responsables de recibir, filtrar y analizar la inteligencia de amenazas. GR.4-5: Se realiza un análisis del impacto potencial de las amenazas emergentes sobre la organización. GR.4-6: La inteligencia de amenazas se utiliza como insumo para el análisis de riesgos de seguridad de la información. Nivel 3: GR.4-7: Se cuenta con un procedimiento documentado sobre el uso de inteligencia de amenazas, abarcando como se recibe, filtra, analiza, clasifica y utiliza la información. GR.4-8: La información de inteligencia de amenazas se utiliza para ajustar o redefinir los controles existentes y apoyar el diseño de nuevos controles para los planes de tratamiento de riesgos. Nivel 4: GR.4-9: Se revisa periódicamente las fuentes confiables de inteligencia identificadas para validar su vigencia. GR.4-10: La organización actualiza sus análisis de riesgos en función de la nueva información derivada del análisis de la inteligencia de amenazas. GR.4-11: Las tendencias identificadas del análisis de la inteligencia de amenazas son utilizadas como insumo para la toma de decisiones estratégicas relacionadas a seguridad.
Guía de implementación	**Identificación de fuentes de inteligencia** La organización debe identificar y documentar fuentes confiables de inteligencia de amenazas relevantes a su contexto operativo y sectorial. Se entiende por inteligencia de amenazas al conocimiento generado a partir del análisis de información sobre actores, eventos, técnicas, vulnerabilidades y patrones de ataque que pueden representar un riesgo para los activos de la organización. Por otra parte, una fuente de

	inteligencia de amenazas es cualquier canal, entidad o mecanismo que provea esta información de forma estructurada y oportuna. Estas pueden incluir organismos oficiales (CERTuy, CSIRT sectoriales), proveedores de servicios de inteligencia, asociaciones sectoriales, comunidades técnicas y fuentes abiertas especializadas. Las fuentes deben revisarse periódicamente para asegurar su vigencia, confiabilidad y pertinencia. **Procesamiento y análisis de la información** Debe establecerse un procedimiento para la recolección, filtrado, análisis y clasificación de la inteligencia de amenazas, que permita identificar su impacto potencial en los activos y procesos críticos de la organización. Este análisis debe integrar variables como criticidad, probabilidad de explotación, contexto organizacional y amenazas conocidas en el ecosistema. El análisis también debe incorporar, dentro de lo posible, indicadores de compromiso (IoC), tácticas, técnicas y procedimientos (TTPs) utilizados por actores de amenaza, vulnerabilidades explotadas y eventos relevantes detectados por las fuentes confiables. Evaluar la necesidad de la contratación de servicios externos de threat intelligence que aporten análisis contextualizados, soporte continuo y capacidades de intercambio automatizado de indicadores de compromiso. **Integración con el análisis de riesgos** La información de inteligencia debe ser considerada como insumo obligatorio en el proceso de evaluación y tratamiento de riesgos de seguridad de la información, así como en la definición de controles preventivos, detección de vectores emergentes y priorización de activos. Toda amenaza relevante identificada debe documentarse y asociarse a evaluaciones de impacto potencial y decisiones de tratamiento de riesgos.
Instituciones de salud	
Instituciones Emisoras de Dinero Electrónico (IEDE)	La organización notificará a las autoridades competentes su participación en los acuerdos de intercambio de información sobre ciberamenazas.
Guía de evidencia para auditoría	• Lista de fuentes de inteligencia utilizadas. • Registros de amenazas recibidas, analizadas y clasificadas. • Programa de capacitación o materiales utilizados para la capacitación. • Registro de tareas y actividades. • Análisis de riesgos que incluya inteligencia de amenazas. • Informe de análisis de impacto de amenazas emergentes. • Actas de revisión de decisiones estratégicas basadas en inteligencia de amenazas.
Normativa asociada	N/A

2.3 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.
Controles	Nivel 1: GH.1-1: Las condiciones laborales del personal, ya sea mediante contrato, estatuto o normativa interna, incluyen cláusulas o disposiciones que establecen sus responsabilidades en materia de seguridad de la información. Nivel 2: GH.1-2: Las responsabilidades del personal respecto a la seguridad de la información están documentadas. GH.1-3: Las responsabilidades en seguridad de la información son comunicadas al personal al momento de su incorporación. Nivel 3: GH.1-4: Existe un procedimiento documentado para la desvinculación del personal que contempla la revocación de accesos físicos y lógicos, y la devolución de activos. GH.1-5: La organización cuenta con un proceso disciplinario formalizado que aplica ante incumplimientos de las políticas de seguridad, de acuerdo con la normativa laboral o administrativa vigente. Nivel 4: GH.1-6: Los documentos contractuales o reglamentarios relacionados con la incorporación y desvinculación del personal se revisan periódicamente para asegurar su vigencia y adecuación. GH.1-7: Se registran y revisan los desvíos e incumplimientos de las obligaciones contractuales relacionadas a seguridad de la información.
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. En los casos de contratos de funcionarios públicos esto se contempla, por ejemplo, en el Decreto 500/991. **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, la devolución de los activos de la organización, 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.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Registros 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. • Plantilla de contrato, estatuto o reglamento con cláusulas de seguridad. • Registro de entrega/aceptación de políticas de seguridad. • Procedimiento de desvinculación formalizado. • Registro de revisión periódica de documentos (contratos, procedimientos). • Registro de desvíos e incumplimientos contractuales. • Documento del proceso disciplinario formal. • Registro de mejora basada en resultados de revisión o incidentes.
Normativa asociada	Ley 19823, Declaración de interés general del código de ética en la función pública Decreto 500/991 Procedimiento administrativo y disciplinario aplicable al funcionario público de la administración central.

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 con las políticas de seguridad de la información de la organización.
Alcance	Cualquier organización.
Controles	Nivel 1: GH.2-1: Se realizan actividades propias de difusión de información relacionada con seguridad de la información, como la difusión de las políticas y mecanismos de protección. Nivel 2: GH.2-2: Se elabora y/o obtiene el material educativo necesario para la realización de las campañas de concientización. GH.2-3: Se elaboran campañas de concientización y/o formación para el personal. GH.2-4: Se planifica un cronograma para la realización de las campañas. Nivel 3: GH.2-5: Las campañas de concientización son aprobadas y se les definen los indicadores de cumplimiento. GH.2-6: Se define un plan de capacitación y entrenamiento en seguridad de la información para todo el personal. Nivel 4: GH.2-7: Se realizan revisiones periódicas de los indicadores de las campañas para verificar su efectividad. GH.2-8: Se evalúa el nivel de conocimiento adquirido por el personal mediante actividades de evaluación periódicas. GH.2-9: Las actividades son aprobadas por el CSI y apoyadas por la Dirección. GH.2-10: El plan es revisado y actualizado periódicamente GH.2-11: Se realizan acciones de mejora a los planes incorporando lecciones aprendidas.
Guía de implementación	**Participación de la Dirección y las Gerencias** 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 deben tener una participación activa en las actividades de concientización. **Plan de concientización y formación** 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. **Materiales de concientización y formación** 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. **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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Acta de aprobación del programa o campañas por el CSI y/o la Dirección. • Cronograma documentado de campañas de concientización. • Indicadores y métricas para medir la efectividad de las campañas. • Plan de concientización y capacitación segmentado por perfiles estratégicos. • Historial de revisión y mejora del plan de concientización. • Evidencia de participación activa de la Dirección en campañas. • Resultados de evaluaciones de conocimiento (pruebas, encuestas, cuestionarios).
Normativa asociada	

Requisito GH.3	Concientizar y formar en materia de seguridad de la información al personal que desempeñan funciones especializadas.
Objetivo	Concientizar y capacitar al personal que desempeña funciones especializadas en materia de seguridad de la información, promoviendo el conocimiento de sus responsabilidades y buenas prácticas conforme a las políticas de seguridad de la información de la organización.
Alcance	Cualquier organización.
Controles	Nivel 1: GH.3-1: Los usuarios privilegiados demuestran conocimiento respecto a la importancia de sus roles y responsabilidades. GH.3-2: El personal de seguridad de la información demuestra concientización respecto a la importancia de sus roles y responsabilidades. GH.3-3: Están definidos los roles y responsabilidades de los interesados externos. Nivel 2: GH.3-4: Se realizan actividades de concientización específicas para usuarios privilegiados con cierta periodicidad. GH.3-5: Se realizan con cierta periodicidad actividades de concientización para el personal de seguridad de la información. GH.3-6: Se realizan actividades de concientización para interesados externos. GH.3-7: La alta gerencia participa de las actividades de concientización. Nivel 3: GH.3-8: Los usuarios privilegiados son capacitados a través de cursos o talleres relevantes adicionales. GH.3-9: El personal de seguridad de la información es capacitado a través de cursos o talleres relevantes adicionales.

	GH.3-10: Se realizan acciones para asegurar que los interesados externos comprendan sus roles y responsabilidades en materia de seguridad de la información. Nivel 4: GH.3-11: El plan de capacitación y entrenamiento en seguridad de la información tiene en cuenta los perfiles e intereses de grupos considerados estratégicos.
Guía de implementación	Se debe considerar todo lo descripto para el requisito GH.2, considerando que el plan de capacitación y entrenamiento en seguridad de la información debe tener en cuenta los perfiles e intereses de grupos considerados estratégicos.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Considerar las evidencias de GH.2, pero validando que estén diferenciadas por perfil (ej.: usuarios privilegiados, personal de seguridad física y de SI).
Normativa asociada	

2.4 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, los sistemas e instalaciones.
Controles	Nivel 1: GA.1-1: Se confecciona y mantiene un inventario de activos físicos del centro de procesamiento de datos, incluyendo servidores, dispositivos de red, racks, UPS y otros componentes relevantes. GA.1-2: Se elabora y mantiene un inventario detallado del software base (ej.: sistemas operativos, servidores de aplicación, servidores de base de datos, hipervisores) y del software de aplicación instalado en los activos del centro de procesamiento de datos. GA.1-3: Cada activo registrado en el inventario debe tener un responsable asignado, cuya información debe estar documentada en el sistema de gestión de activos o inventario utilizado. Nivel 2: GA.1-4: El inventario de activos físicos debe incluir todos los dispositivos utilizados dentro y fuera del centro de procesamiento de datos, tales como estaciones de trabajo (PCs), dispositivos de

	almacenamiento extraíble, impresoras, dispositivos de red, entre otros. GA.1-5: El inventario debe incluir las plataformas de software y aplicaciones implementadas, independientemente de su ubicación física o modalidad (on premise o en la nube). GA.1-6: Se debe llevar un control actualizado del licenciamiento del software instalado, incluyendo información sobre tipo de licencia, vigencia y uso asignado. GA.1-7: El inventario debe estar debidamente documentado y accesible para las personas autorizadas por la organización. Nivel 3: GA.1-8: Las políticas, procesos y procedimientos para la actualización del inventario de activos deben estar formalmente documentados. GA.1-9: La organización debe utilizar una herramienta de software especializada para registrar, seguir y controlar sus activos de información y tecnológicos. GA.1-10: Los procesos y procedimientos de actualización del inventario deben incorporar, total o parcialmente, mecanismos de automatización. GA.1-11: Se debe establecer y mantener un proceso de control y monitoreo continuo del licenciamiento del software, con alertas ante vencimientos o irregularidades. Nivel 4: GA.1-12: Se realizan auditorías internas periódicas para verificar el cumplimiento y alineación de la política y los procedimientos establecidos. GA.1-13: Se elimina el software y/o hardware que esté fuera de soporte o que represente un riesgo no aceptable.
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 e incluyendo los servicios alojados en la nube. 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.
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 necesario que todo aquel equipamiento que procese o almacene información de salud se ubique en el centro de procesamiento 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 procesamiento de datos.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Procedimiento de administración de activos. • Procedimientos o instructivos formales de alta, baja y modificación de activos. • Capturas o informes de la herramienta de inventario utilizada. • Evidencia de automatización en las políticas, procesos y/o procedimientos. • Controles o reportes de licenciamiento de software y su monitoreo continuo. • Registros de auditorías internas.
Normativa asociada	N/A

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.
Controles	Nivel 1: GA.2-1: Están identificados los activos que contienen información crítica para la organización, en base a criterio institucionalmente definido que establezca qué se considera información crítica o sensible. GA.2-2: Cada activo registrado en el inventario debe contar con una etiqueta o atributo que refleje su clasificación según los criterios previamente definidos. Nivel 2:

	GA.2-3: Los activos que almacenan o procesan información deben estar clasificados de acuerdo con los criterios establecidos en el procedimiento de clasificación. GA.2-4: La herramienta de inventario de activos debe permitir registrar, consultar y mantener la clasificación de la información asociada a cada activo. Nivel 3: GA.2-5: Se cuenta con una política y/o procedimiento de clasificación de la información, alineado a la normativa nacional vigente. GA.2-6: Se ha definido un procedimiento para el etiquetado de activos clasificados, que contemple tanto los activos digitales como los físicos. GA.2-7: La clasificación de la información debe estar integrada en todas las etapas del ciclo de vida del activo: alta, modificación, uso y baja. GA.2-8: Las restricciones de acceso deben definirse y aplicarse en función de la clasificación de los activos y el perfil de los usuarios autorizados. Nivel 4: GA.2-9: Se realizan controles internos periódicos para verificar que la clasificación de la información asociada a cada activo sea correcta y vigente.
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; esta identificación podrá contemplar los tipos de datos y metadatos gestionados por la organización. 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.
Instituciones de salud	**Protección de datos personales – datos sensibles** 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 aquellos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley”. **Confidencialidad de los CDA** Las instituciones deben considerar la “Guía CDA Mínimo” para evaluar el nivel de confidencialidad de cada CDA (confidentialityCode) preestableciendo criterios de asignación.

	Instituciones de salud pública Las instituciones de salud pública deben clasificar la información de acuerdo a la ley 18.381. **Instituciones de salud privadas** 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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	Se mantienen los diagramas de flujo de información y del ciclo de pago especificando las condiciones de seguridad implementadas en cada línea de comunicación y los ciclos de pago.
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. • Política y procedimiento de clasificación de información. • Procedimiento para el etiquetado de activos. • Evidencia de uso de herramientas que permitan registrar y gestionar la clasificación (capturas, informes, logs). • Evidencia de controles de acceso basados en clasificación. • Registros de auditorías internas o revisiones periódicas sobre clasificación y acceso.
Normativa asociada	Ley 18.381: Derecho de acceso a la información pública. Ley 18.331: Protección de datos personales, acción de habeas data.

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.
Controles	Nivel 1: GA.3-1: Existen pautas del uso aceptable de los activos de la información. GA.3-2: Toda persona que acceda a activos de información debe aceptar formalmente, previo al acceso, las condiciones de uso establecidas por la organización. Nivel 2: GA.3-3: Se debe restringir el almacenamiento de información sensible en activos que no cuenten con controles adecuados; en caso de ser necesario, se deben aplicar mecanismos de protección como cifrado o control de acceso con MFA. GA.3-4: Se aplican restricciones técnicas o administrativas que limitan acciones no autorizadas sobre los activos, como la

	instalación de software no autorizado o el cambio de configuraciones críticas. Nivel 3: GA.3-5: Está definida formalmente la política sobre el uso adecuado de los activos de la información de la organización. GA.3-6: La política de uso adecuado de los activos es difundida a todo el personal, proveedores y terceros que utilicen activos de información. GA.3-7: Se realiza un control periódico de los activos que contienen o procesan información sensible. GA.3-8: Existe un plan de respuesta en caso de pérdida o robo de los activos de información. Nivel 4: GA.3-9: Las medidas de protección implementadas en los activos informáticos se monitorean de forma proactiva 7x24. GA.3-10: Se realizan evaluaciones periódicas para verificar que el uso de los activos se ajusta a las condiciones establecidas en la política.
Guía de implementación	Se debe definir una política donde se detalle el uso aceptable de los activos, el uso prohibido, responsabilidades, cuando se debe devolver, 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.
Instituciones de salud	En el caso de las instituciones de salud, las pautas de uso aceptable de activos deben incluir al equipamiento médico.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Descripción de los mecanismos de control implementados. • Registros de capacitaciones realizadas, incluyendo temario, fecha, participantes y evaluaciones. • Evidencia de controles periódicos, como informes de monitoreo, o auditorías internas que verifiquen el cumplimiento de las condiciones de uso. • Plan de respuesta ante pérdida o uso indebido, con evidencia de pruebas o simulacros.
Normativa asociada	N/A

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.
Controles	Nivel 1: GA.4-1: Se realiza difusión sobre la importancia de la protección y uso seguro de los medios extraíbles. Nivel 2: GA.4-2: Están identificados y documentados los tipos de medios de almacenamiento externos permitidos para su uso dentro de la organización. GA.4-3: Se encuentran elaboradas y difundidas las pautas para el uso seguro de los medios de almacenamiento externos. GA.4-4: Los medios de almacenamiento externo se encuentran inventariados y clasificados según la clasificación de su información y sus características. Nivel 3: GA.4-5: Están definidas acciones específicas en caso de hurto, pérdida o daño del medio, y se difunde el procedimiento a todos los interesados. GA.4-6: Se encuentra establecida formalmente la política y el procedimiento de gestión de medios de almacenamiento externos. Nivel 4: GA.4-7: Se realizan revisiones de control interno sobre el cumplimiento de las pautas de uso de medios extraíbles, de la política y el procedimiento. GA.4-8: Los resultados de las revisiones son utilizados para la mejora de la política y el procedimiento, se comunican al RSI y demás partes interesadas.
Guía de implementación	Para la implementación de este requisito se deben contemplar medios físicos (por ejemplo: pendrive, disco externo, cintas) y almacenamiento en la nube (por ejemplo: Dropbox, Google Drive). **Procedimiento para el manejo de medios de almacenamiento externos.** 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. **Inventario de medios de almacenamiento externos** 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. **Controles en medios de almacenamiento externos** 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. **Medidas de protección** Si existen medios en reposo con información sensible, junto a otro tipo de información, el dispositivo debe ser considerado como contenedor de información sensible (por ejemplo, información de salud) y, por tanto, deberá ser considerado con las mismas medidas que la organización haya establecido para ese tipo de información, debiendo cumplir mínimamente con pautas de cifrado de la información.
Instituciones de salud	Se debe contemplar la definición de controles tendientes a mitigar el riesgo del almacenamiento de información sensible en diversos tipos de 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 debe contar con una política para la gestión de la información que se encuentra almacenada dentro de los dispositivos biomédicos.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. ● Política para la gestión de los medios de almacenamiento externos. ● 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. • Casos documentados de pérdidas, robos o incidentes y acciones tomadas. • Informes de revisión interna sobre cumplimiento del procedimiento. • Comunicaciones internas o registros de difusión a usuarios. • Evidencia de mecanismos de protección como cifrado y autenticación MFA.
Normativa asociada	Ley 18.331: Protección de datos personales, acción de habeas data.

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.
Controles	Nivel 1: GA.5-1: Están definidas las pautas para la disposición final y borrado seguro de medios de almacenamiento. GA.5-2: Está difundida la importancia de la eliminación de medios de almacenamientos que ya no serán utilizados. Nivel 2: GA.5-3: Están definidos responsables o ubicaciones específicas para la eliminación segura de medios de almacenamiento. GA.5-4: Están establecidos los criterios para determinar cuándo corresponde la destrucción lógica y/o física de la información. Nivel 3: GA.5-5: Está definida formalmente una política de destrucción de la información. GA.5-6: Está definido formalmente un procedimiento de destrucción de la información. GA.5-7: Se registran las actividades de destrucción de la información, incluyendo fecha, tipo de medio, método aplicado y personal. GA.5-8: Se verifica la efectividad de los métodos de destrucción utilizados. Nivel 4: GA.5-9: Se realizan actividades de control interno para evaluar la correcta aplicación del procedimiento de destrucción.
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.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Política de destrucción de información y medios de almacenamiento. • Procedimiento operativo para la destrucción segura de medios de almacenamiento. • Registros de destrucción por período auditado (formularios, actas, informes, etc.). • Comunicación institucional sobre las pautas de destrucción a usuarios finales. • Resultados de controles internos y documentos que demuestren el cierre de desvíos detectados. • Evidencia de verificación de efectividad de los métodos utilizados (por ejemplo, pruebas de borrado, certificados de destrucción por terceros). • Listas de control de medios destruidos, integradas con inventario previo.
Normativa asociada	Ley 18.331: Protección de datos personales, acción de habeas data.

2.5 Control de acceso

Requisito CA.1	Gestión de identidades y credenciales
Objetivo	Establecer procesos centralizados, seguros y auditables para gestionar el ciclo de vida de las identidades digitales y sus credenciales, incluyendo la creación, modificación, autenticación y baja de cuentas de usuario, asegurando su correcta asociación con funciones y responsabilidades, como base del control de acceso lógico.

Controles	Nivel 1: CA.1.1: Todos los sistemas requieren autenticación. CA.1-2: El acceso a la red y los sistemas debe realizarse con usuarios nominados. CA.1-3: El uso de usuarios privilegiados se encuentra controlado. CA.1-4: Los accesos a aplicaciones se realizan utilizando mecanismos de autenticación seguros. Nivel 2: CA.1-5: El uso de usuarios genéricos debe estar fundamentado y autorizado por excepción. CA.1-6: Existen pautas definidas para la realización de altas, bajas y modificaciones de acceso lógico que además incluyen aprobaciones. CA.1-7: Se identifican los casos que requieren autenticación fuerte y se determinan los controles requeridos. CA.1-8: Las credenciales de autenticación (contraseñas, certificados, tokens, biometría) están protegidas en reposo y en tránsito mediante mecanismos criptográficos robustos. Nivel 3: CA.1-9: Se define una política de gestión de usuarios y contraseñas, y se instruye al personal para su uso correcto. CA.1-10: Se cuenta con un procedimiento para el ABM de usuarios. CA.1-11: La gestión de identidades y credenciales se realiza en forma centralizada, al menos en forma administrativa. CA.1-12: Los tokens o credenciales utilizadas para el acceso (por ejemplo, SAML assertions, JWTs) se validan en cada acceso y su integridad es verificada. Nivel 4: CA.1-13: Se establecen procesos de revisiones y auditorías continuas para verificar que las redes, sistemas, recursos y dispositivos están funcionando con la autenticación y configuración requerida y acordada por la organización. CA.1-14: La política y procedimientos son revisados periódicamente.
Guía de implementación	**Procesos de gestión de identidades digitales** La organización debe establecer procedimientos centralizados para administrar el ciclo de vida de las identidades digitales, abarcando la creación, modificación, suspensión y baja de cuentas de usuario. Cada cuenta debe asociarse inequívocamente a una persona, función o servicio autorizado, permitiendo así la asignación de permisos y privilegios según las responsabilidades asignadas. El acceso a sistemas y redes se debe conceder únicamente a través de usuarios nominados y validados, prohibiéndose por defecto el uso de cuentas genéricas, salvo excepciones debidamente justificadas y documentadas. **Control y uso de cuentas privilegiadas** El uso de cuentas con privilegios elevados debe encontrarse acotado a situaciones justificadas y bajo una estricta supervisión. Estas cuentas deberán tener credenciales diferenciadas de las cuentas de uso habitual y estar sujetas a controles que permitan identificar y auditar todas las acciones realizadas bajo dichas identidades. Las revisiones periódicas

	sobre el uso y la vigencia de estas cuentas son indispensables para detectar y corregir posibles desviaciones. **Mecanismos de autenticación segura y protección de credenciales** Los mecanismos de autenticación seguros son los métodos y procesos que se utilizan para verificar la identidad de un usuario, dispositivo o sistema de una manera fiable y resistente a los ataques. El objetivo principal es garantizar que solo las entidades autorizadas puedan acceder a datos, sistemas o recursos protegidos. Por ejemplo: múltiples factores de autenticación, contraseña de un solo uso, autenticación biométrica, entre otros. Todos los accesos a los sistemas y recursos de la organización deben realizarse mediante mecanismos de autenticación segura que garanticen la individualización de los usuarios. Se debe usar la autenticación multifactor especialmente para accesos remotos, aplicaciones o servicios críticos o que manejen información sensible. Las credenciales asociadas a las identidades digitales (contraseñas, certificados, tokens, etc.) deben protegerse tanto en reposo como en tránsito utilizando tecnologías criptográficas robustas y procedimientos que eviten su divulgación o reutilización indebida. Los sistemas que utilicen tokens de acceso o credenciales temporales deben validar su integridad y vigencia en cada autenticación. **Política y procedimientos de gestión de usuarios y contraseñas** Se debe formalizar una política de gestión de identidades y credenciales que contemple los requisitos mínimos para la creación de cuentas, el proceso de autorización de nuevos accesos, la modificación o revocación de privilegios, y los mecanismos para la baja segura de usuarios. Los procedimientos asociados deben incluir la aprobación documentada de cada acción relevante, el registro detallado de los cambios realizados y la notificación a las partes interesadas. Es fundamental que la administración de estos procesos se realice de manera centralizada para facilitar el control y la trazabilidad. **Métodos de autenticación y verificación de identidad** • En aquellos casos que se requiera una autenticación fuerte y verificación de identidad se podrá establecer la utilización de métodos alternativos como: eID (cédula electrónica), token, autenticación multifactor, entre otros. • En otros casos se puede considerar la autenticación adaptativa, también conocida como autenticación basada en riesgo (RBA), evaluando en cada caso el contexto de la conexión para decidir si debe permitir el acceso, bloquearlo o solicitar una prueba de identidad adicional. **Definición de cuentas de usuario y control interno**

	• 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 deben 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. • Restricciones para acceso remoto a información confidencial. • Al acceder a información confidencial desde ubicaciones remotas, se deben definir controles específicos. Por ejemplo, podría considerarse restringir acciones como copiar, mover, imprimir, utilizar capturas de pantalla o almacenar información en discos duros locales y medios electrónicos extraíbles, a menos que exista una autorización explícita y con una necesidad justificada. **Revisión, auditoría y mejora continua** La organización debe realizar auditorías periódicas para verificar que todas las identidades y credenciales activas correspondan a usuarios vigentes y autorizados, y que los controles implementados sigan siendo efectivos frente a las amenazas emergentes. Se recomienda establecer revisiones automáticas o manuales sobre los accesos concedidos, la configuración de autenticación y los privilegios asignados. Los resultados de estas auditorías deben utilizarse para actualizar procedimientos, corregir desvíos y fortalecer la seguridad en la gestión de identidades digitales.
Instituciones de salud	**Acceso lógico a dispositivos médicos** Dentro de la política de gestión de usuarios y contraseñas 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. **Identificación y autenticación** 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.”. **Gestión de accesos** 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, debe ser mediante doble factor de autenticación.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Política de gestión de usuarios y contraseñas. • Mecanismos de autenticación utilizados. • Controles aplicados para el acceso remoto a información confidencial. • 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

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).
Controles	Nivel 1: CA.2-1: La revisión de privilegios se realiza en forma reactiva frente a un cambio o baja, al menos para los sistemas críticos. Nivel 2:

	CA.2-2: Está establecida la periodicidad con la que se realizan las revisiones de los privilegios y la validez de las cuentas asociadas. CA.2-3: Están definidos los responsables de la revisión de privilegios y de la validez de las cuentas en cada sistema. CA.2-4: Se mantiene un inventario de usuarios con permisos y privilegios elevados, validando también la vigencia de las cuentas. Nivel 3: CA.2-5: Existe una política de control de acceso lógico donde se estipula la revisión de privilegios periódicamente a todos los usuarios y en todos los sistemas. CA.2-6: Existen y se aplican procedimientos formales de revisión de permisos que abarcan todo el ciclo de vida (alta, baja y modificación) de los usuarios, incluyendo los privilegiados. CA.2-7: Se realizan revisiones de los derechos de acceso de los usuarios y se cuenta con registro de tales acciones. CA.2-8: Se documentan los resultados de cada revisión y se comunican al RSI, a las gerencias y demás partes interesadas. Nivel 4: CA.2-9: El resultado de las revisiones se comunica formalmente a las gerencias y otras partes interesadas. CA.2-10: Se realizan auditorías internas sobre el cumplimiento del procedimiento de revisión de privilegios y la política de control de acceso lógico, en específico de su apartado de revisiones periódicas.
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.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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

Requisito CA.3	Establecer controles criptográficos.
Objetivo	Proteger la confidencialidad, autenticidad e integridad de la información en soporte digital.
Controles	Nivel 1: CA.3-1: Se identifican los datos históricos y respaldos que deben ser protegidos mediante mecanismos seguros. Nivel 2: CA.3-2: Los respaldos y/o datos históricos fuera de línea se almacenan en forma cifrada. Nivel 3: CA.3-3: Se documentan los mecanismos criptográficos implementados. CA.3-4: Está definida una política de uso de controles criptográficos. CA.3-5: Se determinan los responsables de la generación de las claves que abarca todo su ciclo de vida. Nivel 4: CA.3-6: Se realizan revisiones periódicas sobre los controles criptográficos utilizados para asegurar la protección de los datos. CA.3-7: Los resultados de estas revisiones son registrados e informados al RSI.
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 o lineamientos sobre el uso de controles criptográficos, la misma debe incluir los lineamientos de protección para la información en tránsito y abarcar los respaldos y datos históricos. • 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. Las claves criptográficas que protegen los tokens de acceso se generan, gestionan y protegen contra la divulgación y el uso indebido. **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). En particular se debe asegurar todas las

	transacciones en línea que involucren datos confidenciales o datos personales identificables. ● Establecimiento de VPN para acceso remoto.
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, y los datos en reposo, relacionados con datos de salud deben estar cifrados.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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

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.
Controles	Nivel 1: CA.4-1: La organización identifica los sistemas y procesos que requieren firma electrónica avanzada. CA.4-2: Los sistemas con firma electrónica utilizados por la organización soportan el uso de certificados electrónicos X.509v3 emitidos por prestadores acreditados ante la UCE. CA.4-3: Se utilizan protocolos seguros y actualizados, evitando tecnologías criptográficas obsoletas o vulnerables. CA.4-4: Deben utilizarse los estándares de codificación de firmas propios de los tipos de documentos firmados (XADES, PDFSignature, etc.). CA.4-5: Se debe hacer la validación de certificados a través de OCSP (Online Certificate Status Protocol), CRL (Certificate Revocation List) o equivalente. Nivel 2: CA.4-6: La solución incorpora medidas de detección de firmas alteradas o invalidadas, incluyendo trazabilidad del error. Nivel 3:

	CA.4-7: La organización documenta un procedimiento técnico y funcional para la implementación de firma electrónica avanzada. CA.4-8: Los sistemas deben soportar el uso de dispositivos criptográficos dedicados en todos los casos de uso de todos los prestadores de Firma Electrónica Avanzada acreditados por la UCE. CA.4-9: La firma digital está embebida en todos los procesos de la organización que la requieren, de modo que los usuarios pueden firmar o validar firmas en el contexto de cada sistema. Nivel 4: CA.4-10: Los sistemas deben permitir el uso de sellos de tiempo compatibles con RFC 3161. CA.4-11: Se realizan auditorías de los módulos de firma electrónica, incluyendo pruebas de cumplimiento de formatos, protocolos, protección de claves y servicios de sellado de tiempo. CA.4-12: Los resultados de las auditorías o revisiones son analizados e incorporados a la mejora de la solución y comunicados al RSI.
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. <u>Contexto de aplicación</u>: 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. • Se debe implementar una solución (posiblemente integración mediante API a firma.gub.uy) para integrar la posibilidad de firmar utilizando cualquier prestador de firma electrónica avanzada uruguaya en forma embebida, así como también para la validación de firmas digitales. 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). Es importante aclarar que, a la fecha de publicación de esta guía, *firma.gub.uy* a través de API está disponible solamente para el sector público.
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. La recomendación para el punto a) es que cada médico utilice la firma electrónica avanzada de persona física para firmar los documentos clínicos. La autenticación con usuario nominado al sistema no es válida como método de firma. Para cumplir el punto c) es necesario validar la vigencia del certificado al momento de la firma y validar la correspondencia de la institución en el certificado y en la firma del CDA.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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.

Requisito CA.5	Segregación de funciones en el acceso lógico
Objetivo	Implementar para el acceso lógico una segregación clara de funciones entre los roles críticos dentro de la organización, previniendo así conflictos de interés y reduciendo el riesgo de manipulación no autorizada de la información y los sistemas.
Controles	Nivel 1: CA.5-1: Están implementados controles que impiden que un mismo usuario solicite, apruebe y asigne accesos en los sistemas críticos. CA.5-2: La asignación de privilegios es ejecutada por un responsable distinto al que la aprueba. Nivel 2: CA.5-3: Se aplican mecanismos preventivos para evitar su asignación conjunta, salvo justificación formal y aprobación excepcional de roles en conflicto. CA.5-4: Está limitada la cantidad de usuarios con privilegios administrativos, siguiendo criterios establecidos. CA.5-5: La segregación de funciones abarca también los diferentes entornos de la organización, evitando que una persona realice actividades en más de un entorno al menos de que esté debidamente justificado y documentado. CA.5-6: El personal de administración de accesos no es el mismo que el que realiza la auditoría sobre dichos accesos. Nivel 3: CA.5-7: Están identificados, documentados y gestionados los posibles conflictos entre roles o combinaciones de privilegios. CA.5-8: Están definidos y documentados los criterios para autorizar privilegios administrativos. CA.5-9: Están definidos y documentados los criterios para determinar cuántos usuarios con privilegios de administrador deben existir por sistema o entorno. CA.5-10: La segregación de funciones está incluida en el procedimiento formal de control de acceso lógico. Nivel 4: CA.5-11: Se audita periódicamente el cumplimiento del procedimiento de segregación de funciones. CA.5-12: En caso de identificarse desviaciones se documentan, y se realizan acciones correctivas con responsables asignados.
Guía de implementación	La autorización de acceso debe ser gestionada de manera segregada, distribuyendo responsabilidades como solicitudes de acceso, aprobaciones y provisión entre varios individuos o grupos. Esto evita concentraciones de poder y el potencial abuso de los privilegios de acceso. La segregación de funciones debe ser acompañada de procesos de auditoría y supervisión robustos, para minimizar el riesgo de que los activos de información sufran modificaciones no autorizadas.

	Es fundamental limitar el número de administradores al mínimo necesario, basándose en las responsabilidades y roles específicos de cada usuario, para reducir los riesgos asociados con el acceso a información crítica. El personal de seguridad que administra los controles de acceso debe estar separado de las funciones de auditoría de estos controles, para mantener una supervisión objetiva. Las responsabilidades de desarrollo, pruebas, garantía de calidad y producción deben estar claramente divididas entre diferentes equipos o individuos, asegurando una independencia que previene conflictos de interés y fortalece la seguridad de los procesos operativos.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Política de control de acceso lógico. • Procedimiento de revisión de privilegio de acceso. • Listado de usuarios con acceso privilegiado. • Listado de conflictos entre roles o combinaciones de privilegios. • 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). • 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.
Normativa asociada	N/A

Requisito CA.6	Gestión de accesos y permisos
Objetivo	Definir, aplicar y revisar los permisos, derechos y autorizaciones de acceso lógico a sistemas, redes, aplicaciones y activos de información; conforme a las políticas de seguridad, aplicando los principios de mínimo privilegio, con trazabilidad, revisión periódica y cumplimiento normativo.
Controles	Nivel 1: CA.6-1: Los derechos de acceso son otorgados con autorización previa. Nivel 2: CA.6-2: El uso de dispositivos externos requiere identificación (inventariado y responsable) y autentificación (permiso de acceso por el rol del usuario o algún otro método). CA.6-3: Las autorizaciones de derechos de acceso son registradas. CA.6-4: El acceso a los activos de información identificados como críticos debe requerir autenticación con múltiple factor (MFA). Nivel 3: CA.6-5: Se aplica el principio de menor privilegio para la asignación de permisos.

	CA.6-6: Se define un procedimiento de acceso lógico a redes, recursos y sistemas de información. CA.6-7: Se define una política de acceso lógico a redes, recursos y sistemas de información. CA.6-8: Las medidas implementadas para el acceso están directamente asociadas al análisis de riesgos sobre el acceso a la información. CA.6-9: La política de acceso lógico incluye el uso de usuarios privilegiados. Nivel 4: CA.6-10: Durante las revisiones continuas de acceso, se verifica y documenta el cumplimiento de las políticas internas, normas, estándares y regulaciones aplicables en materia de protección de datos y privacidad de la información.
Guía de implementación	**Definición y autorización de permisos de acceso** La organización debe asegurar que todos los derechos, permisos y autorizaciones de acceso a sistemas, redes, aplicaciones y activos de información sean previamente definidos y formalmente autorizados, de acuerdo a las políticas de seguridad vigentes. El otorgamiento de permisos debe estar respaldado por un proceso documentado, asegurando que cada acceso otorgado responda a una necesidad justificada y esté alineado a las funciones y responsabilidades del usuario o servicio involucrado. Toda autorización debe ser registrada para garantizar la trazabilidad y la posterior revisión de los accesos. **Aplicación del menor privilegio** El acceso lógico y los permisos otorgados deben seguir estrictamente el principio de mínimo privilegio, garantizando que cada usuario cuente únicamente con los derechos indispensables para el cumplimiento de sus tareas. Las autorizaciones y cambios en los derechos de acceso deben ser documentados y actualizados de forma centralizada. **Procedimientos y política de acceso lógico** La política de control de acceso lógico establece los lineamientos generales que debe seguir la organización para gestionar y proteger el acceso a los activos de información. Su objetivo es asegurar que únicamente las personas autorizadas puedan acceder, y solo a la información mínima necesaria para cumplir con sus funciones. Para ello, la organización debe contar con mecanismos formales de autorización, así como procedimientos definidos para la solicitud, aprobación, revocación y notificación de accesos. Además, debe establecerse un proceso para la gestión de accesos de terceros, el cual debe estar respaldado por acuerdos específicos aprobados por la Dirección o quien ésta designe. **Gestión de accesos privilegiados y autenticación reforzada** La política de acceso lógico debe contemplar el uso diferenciado y la gestión rigurosa de los usuarios privilegiados, estableciendo controles específicos para su uso, revisión y auditoría. Para los activos de

	información identificados como críticos, se debe exigir el uso de autenticación con múltiple factor (MFA), reforzando así el nivel de seguridad sobre estos recursos y minimizando el riesgo de accesos no autorizados. **Revisión, cumplimiento normativo y mejora continua** La organización debe establecer mecanismos para la revisión continua de los accesos y permisos otorgados, considerando las políticas, normas, estándares y regulaciones aplicables en materia de protección de datos y privacidad de la información. Las revisiones periódicas deben identificar accesos innecesarios, cuentas obsoletas o privilegios excesivos, permitiendo su corrección oportuna. Los procesos de auditoría y revisión deben estar documentados, y sus resultados deben alimentar acciones de mejora y la actualización de políticas y procedimientos para asegurar el cumplimiento normativo y la eficacia de los controles implementados.
Instituciones de salud	**Acceso lógico a dispositivos médicos** 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. **Trazas o logs** 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.". **Gestión de accesos** 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. **Mínimo privilegio para terceros** El acceso concedido a terceros a información sensible, como la Historia Clínica Electrónica (HCE), debe ser estrictamente limitado al mínimo necesario y restringido en duración, revocándose tan pronto como deje de ser necesario. Todas las conexiones remotas con

	terceros deben asegurarse mediante canales encriptados para proteger la transmisión de información.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Política de control de acceso lógico. • Política de gestión de usuarios y contraseñas. • Mecanismos de autenticación utilizados. • Controles aplicados para el acceso remoto a información confidencial. • 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

2.6 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 (por ejemplo, recinto donde se almacenan los respaldos) y proteger las instalaciones y equipos contra robos, daños o mal uso.
Alcance	Cualquier organización.
Controles	Nivel 1: SF.1-1: Están identificadas las áreas que requieren control de acceso físico. SF.1-2: Están implementados los controles de acceso físico a las instalaciones de los centros de procesamiento de datos. SF.1-3: Se gestionan (evalúan, autorizan y registran) las autorizaciones de acceso al centro de procesamiento de datos. Nivel 2:

	SF.1-4: Están establecidos perímetros de seguridad en el centro de procesamiento de datos y las áreas seguras. SF.1-5: Están implementados controles de acceso físico para otras áreas definidas como seguras. SF.1-6: Se gestionan (evalúan, autorizan y registran) las autorizaciones de acceso a las áreas definidas como seguras. SF.1-7: Se lleva un registro de accesos físicos al centro de procesamiento de datos y áreas seguras. Nivel 3: SF.1-8: Existe una política de control de acceso físico formalmente aprobada. SF.1-9: Se revisan de forma reactiva los registros de acceso a las diferentes áreas. SF.1-10: Las aplicaciones que manejan información sensible requieren reautenticación periódica, especialmente cuando se accede desde ubicaciones de alto riesgo. Nivel 4: SF.1-11: Está establecido un procedimiento de revisión periódica de los accesos al centro de procesamiento de datos y a las áreas seguras. SF.1-12: Se realizan actividades de control interno para verificar el cumplimiento de los procedimientos establecidos. SF.1-13: Se aplican controles de tiempo de conexión y condiciones de acceso desde ubicaciones públicas o externas a la organización.
Guía de implementación	**Aclaraciones sobre arquitectura y estructura** 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 procesamiento 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. **Aclaraciones sobre acceso físico** 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 procesamiento de datos. El acceso al Centro de procesamiento 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 procesamiento 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. **Política de control de acceso físico y procedimientos** Se debe contar con una política de control de acceso físico e implementar todos los procedimientos que se entiendan necesarios para su implementación. **Registro de accesos físicos** 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 procesamiento de datos y áreas relacionadas o seguras deben revisarse en forma periódica y el procedimiento de revisión debe estar documentado. En los casos donde el centro de procesamiento de datos sea en la nube, todos los controles deberán estar cubiertos por el proveedor, debiendo presentar certificaciones o constancias que avalen esto.
Instituciones de salud	**Perímetros** 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. **Política de control de acceso físico** En la política de control de acceso físico, se debe contemplar el control de acceso al equipamiento médico.

	Dispositivos médicos móviles 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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. ● Políticas y procedimientos de seguridad necesarios que incluyan manejo de equipos sin supervisión. ● Procedimiento de revisión de accesos físicos al centro de procesamiento de datos y áreas seguras. ● Registros de actividades de control interno de los procedimientos.
Normativa asociada	

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.
Controles	Nivel 1: SF.2-1: Están identificados los riesgos ambientales que pueden afectar al centro de procesamiento de datos. SF.2-2: Existen medidas de control del medio ambiente físico en los centros de procesamiento de datos. Nivel 2: SF.2-3: Están instalados sistemas de detección y extinción de incendios con mantenimiento periódico. SF.2-4: Se implementan herramientas automatizadas que apoyan el monitoreo de los controles relacionados al medio ambiente físico. SF.2-5: Está implementado un sistema de climatización que regula la temperatura y humedad. Nivel 3: SF.2-6: La política de seguridad del equipamiento incluye medidas ambientales.

	SF.2-7: Se cuenta con un procedimiento documentado de monitoreo de los controles ambientales. Incluye el uso de herramientas automatizadas. Nivel 4: SF.2-8: Los controles ambientales se revisan periódicamente y se ajustan según las nuevas condiciones climáticas y tecnológicas. SF.2-9: Se realizan actividades de control interno para verificar el cumplimiento de la política y procedimientos asociados. SF.2-10: Los resultados del monitoreo son utilizados para la realización de las lecciones aprendidas, las mismas son utilizadas para mejorar los procedimientos relacionados.
Guía de implementación	**Aclaraciones sobre los controles ambientales** 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, el fuego no debe traspasar la barrera física del centro de procesamiento 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 procesamiento 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. En los casos donde el centro de procesamiento de datos sea en la nube, todos los controles deberán estar cubiertos por el proveedor, debiendo presentar certificaciones o constancias que avalen esto.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	
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. • Procedimiento de monitoreo de los controles ambientales. • Política de seguridad del equipamiento. • Registros de actividades de control interno del procedimiento.
Normativa asociada	

Requisito SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento.
Objetivo	Lograr una adecuada administración de los componentes críticos alojados en sitios o centros de procesamiento de datos.
Alcance	Cualquier organización
Controles	Nivel 1: SF.3-1: Se monitorea de forma reactiva o esporádica los sistemas o servicios más críticos. SF.3-2: Se registran los logs de las fallas y alertas críticas, y se conserva su historial para revisión. Nivel 2: SF.3-3: Se monitorea de forma automatizada los activos críticos del centro de procesamiento de datos, generando alertas ante la detección de problemas. SF.3-4: Existen funciones integradas en los dispositivos que permiten el monitoreo de las amenazas típicas (alimentación eléctrica, enfriamiento, etc.). SF.3-5: Se definen notificaciones de alertas (correo, SMS, etc.) al personal designado. Nivel 3: SF.3-6: En el centro de procesamiento de datos se implementan alertas sobre anomalías que podrían transformarse en problemas para los activos críticos. SF.3-7: Las alertas notifican cuando se comienzan a dar las casuísticas que pueden derivar en un incidente aún no concretado. SF.3-8: Establecer un procedimiento documentado de monitoreo que incluye el uso de herramientas automatizadas. Nivel 4: SF.3-9: Se envían alertas del estado de los componentes prioritarios para el funcionamiento de la organización ante los cambios de entorno. SF.3-10: Se monitorean todos los activos de información del centro de procesamiento de datos, con cruzamiento de información de diversas fuentes, contemplando, entre otros, alertas preventivas y reactivas. SF.3-11: Se cuenta con un proceso de control interno para la verificación de cumplimiento de los procedimientos de monitoreo del centro de procesamiento de datos.
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** Este establece la recomendación de contar con un sistema de gestión y monitoreo centralizado que pueda alertar fallas en componentes críticos del centro de procesamiento de datos. **Aclaraciones sobre el sistema de gestión y monitoreo** Para administrar correctamente un centro de procesamiento 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 procesamiento 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. **Herramientas de monitoreo** 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. **Monitoreo alternativo** Se debe contar con alternativas de monitoreo (al menos manual) ante fallas del mecanismo principal.
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.

Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Herramientas utilizadas para el monitoreo. • Procedimiento de monitoreo. • 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.
Normativa asociada	

Requisito SF.4	Seguridad del equipamiento
Objetivo	Proteger el equipamiento, tanto dentro como fuera de los centros de datos, mediante la definición de controles, políticas y procedimientos de operación segura y acceso controlado.
Controles	Nivel 1: SF.4-1: Todos los dispositivos con información sensible disponen de barreras físicas que impiden su extracción o manipulación no autorizada (cerraduras, tapas de seguridad, sensores de apertura, etc.). SF.4-2: Al recibir equipos nuevos se inspeccionan, y documenta el estado de los sellos o empaques de fábrica, registrando cualquier indicio de apertura o daño. Nivel 2: SF.4-3: Se deshabilitan los puertos no utilizados (USB, serie, módulos de expansión, etc.) en los dispositivos del centro de procesamiento de datos. SF.4-4: Se instalan sellos o cintas de seguridad con código único en los puntos de acceso al interior de los chasis, de manera que cualquier manipulación quede registrada. SF.4-5: Los dispositivos de usuario final están configurados para bloquear automáticamente la sesión tras un máximo de 15 minutos, o menos, de inactividad. SF.4-6: Se implementa el cierre automático de sesión después de 30 minutos sin actividad, o menos, en los dispositivos de usuario final. Nivel 3: SF.4-7: Esta formalmente definida una política de seguridad del equipamiento que establece lineamientos para la protección física, manejo cuando esté los equipos estén sin supervisión, entre otros puntos. SF.4-8: Existe un procedimiento documentado de respuesta a eventos de manipulación detectada, que incluye la investigación inicial y evaluación de posibles compromisos de integridad. SF.4-9: Existe un procedimiento documentado para la seguridad del equipamiento, que describa las configuraciones preventivas y las acciones de respuesta ante incidentes o situaciones de riesgo,

	incluyendo escenarios como la detección de equipos sin supervisión. Nivel 4: SF.4-10: Se cuenta con un proceso de control interno para verificar el cumplimiento de los procedimientos de seguridad del equipamiento y documentar hallazgos. SF.4-11: Se realiza una revisión periódica de los procedimientos y de las medidas de seguridad implementadas en el equipamiento, incorporando ajustes derivados de incidentes, no conformidades y oportunidades de mejora.
Guía de implementación	**Acceso a equipos desatendidos** Se debe informar a todos los usuarios acerca de las políticas y procedimientos de seguridad necesarios para el manejo adecuado de equipos desatendidos. Esto incluye la obligación de finalizar sesiones activas al concluir sus tareas, utilizando mecanismos de bloqueo eficientes, tales como el uso de contraseñas. Además, se deben configurar para realizar el bloqueo de sesión automática en caso de inactividad. Esto se complementa con la ocultación de información visible en la pantalla mediante un protector de pantalla, el cual se activa tras 15 minutos de inactividad y cierre de sesión automático después de 30 minutos sin actividad. Por último, se implementan controles de tiempo de conexión, incluyendo intervalos de tiempo predeterminados y la necesidad de reautenticación periódica para aplicaciones que manejen datos sensibles, utilizadas desde ubicaciones de alto riesgo, como áreas públicas o externas fuera del control de seguridad de la organización. **Política de seguridad del equipamiento** 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.
Instituciones de salud	**Seguridad del equipamiento de los centros de datos y equipamiento médico** 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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-

Guía de evidencia para auditoría	• Registro de deshabilitación de puertos no utilizados (USB, serie, módulos de expansión) en los dispositivos del centro de procesamiento de datos (checklists, informes técnicos o fotografías). • Inventario de dispositivos sensibles con detalle de barreras físicas implementadas (cerraduras, tapas de seguridad, sensores de apertura). • Actas o registros de recepción de equipos nuevos, inspección de sellos/empaques y reporte de cualquier anomalía. • Configuraciones de bloqueo automático de sesión y cierre automático por inactividad en dispositivos de usuario final (políticas, capturas de pantalla, evidencia técnica). • Política de seguridad del equipamiento formalmente aprobada y difundida. • Procedimiento documentado de respuesta ante eventos de manipulación detectados. • Registros de revisiones y auditorías internas sobre cumplimiento de los procedimientos de seguridad del equipamiento.
Normativa asociada	

Requisito SF.5	Establecer el mantenimiento de los componentes críticos.
Objetivo	Asegurar la disponibilidad y vida útil del equipamiento mediante mantenimiento preventivo y/o correctivo, planificado y controlado.
Controles	Nivel 1: SF.5-1: Se gestiona y/o realiza el mantenimiento sobre los activos del centro de procesamiento de datos. SF.5-2: Se aprueba el alta y baja de los usuarios que realizan mantenimiento de forma remota a los activos informáticos del centro de procesamiento de datos. Nivel 2: SF.5-3: Se establecen planes de mantenimiento para las dependencias de los componentes críticos. SF.5-4: Se establecen los planes anuales de mantenimiento. SF.5-5: Se gestiona el acceso a los usuarios autorizados para realizar las tareas de mantenimiento programado. Nivel 3: SF.5-6: El RSI realiza la gestión de aprobación de los usuarios para conexión remota a los sistemas y activos de la organización, cumpliendo con el plan anual de mantenimiento. SF.5-7: Existe una política y/o procedimiento documentado de mantenimiento (criterios de prioridad, coordinación con operación, pruebas de validación y comunicación de resultados). Nivel 4: SF.5-8: Existe un proceso de control interno para verificar el cumplimiento del procedimiento de mantenimiento y la calidad

	de la documentación asociada. SF.5-9: Tras cualquier mantenimiento en el que se detecten desviaciones o incidentes, se elabora un registro formal de lecciones aprendidas que incluya la descripción de lo ocurrido, el análisis de causas, las acciones correctivas adoptadas y la actualización de los procedimientos afectados.
Guía de implementación	**Política de mantenimiento de los activos** Se debe contar con una política de mantenimiento del equipamiento que establezca objetivos, alcance, roles y responsabilidades, tipos de mantenimiento (preventivo, correctivo y de emergencia), y criterios de priorización por criticidad del servicio. La política debe contemplar tanto el equipamiento ubicado dentro del centro de procesamiento de datos como fuera del mismo, e incluir el relacionamiento con terceros (proveedores y servicios técnicos). **Clasificación y priorización** El mantenimiento debe planificarse considerando la criticidad de los activos y su impacto en los servicios de la organización. A igualdad de condiciones, se priorizarán los equipos vinculados a procesos críticos y aquellos cuyo tiempo de indisponibilidad pueda afectar objetivos regulatorios o contractuales. La priorización debe estar documentada y revisarse al menos una vez al año. **Plan de mantenimiento** Se debe definir un plan que permita establecer las acciones preventivas y correctivas de todo el equipamiento que se encuentre fuera de los centros de datos, principalmente los equipos de los usuarios finales, 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. **Gestión de accesos para mantenimiento** Previo a cada intervención, se debe autorizar el acceso de técnicos internos o externos, habilitando cuentas temporales y con privilegios mínimos estrictamente necesarios. El acceso debe quedar registrado (fecha/hora, persona, tarea, activo intervenido). Para personal externo, se deben contemplar acuerdos de confidencialidad y, cuando aplique, acompañamiento o supervisión del personal de la organización. **Mantenimiento correctivo y de emergencia** Se debe definir un flujo abreviado para tareas correctivas y emergencias, con criterios de activación, responsables de aprobación rápida y comunicación a las áreas afectadas. Finalizada la intervención, se documentará el incidente, se validará el servicio y se realizará un breve análisis de causa raíz para determinar acciones preventivas.

	Registros y trazabilidad Cada tarea debe generar un registro con: número de orden, fecha y hora, personal interviniente, descripción de actividades, activos afectados, repuestos utilizados, resultados de pruebas, reposición de sellos/barreras y validación del servicio. La documentación debe ser suficiente para reconstruir la intervención y respaldar auditorías.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Plan anual de mantenimiento aprobado y actualizado. • Listado de usuarios autorizados para tareas de mantenimiento programado y registros de accesos. • 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. • Registros de mantenimiento realizados sobre activos del centro de procesamiento de datos (planillas, órdenes de trabajo, reportes de proveedores).
Normativa asociada	

2.7 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.
Controles	Nivel 1: SO.1-1: El software de base y aplicaciones críticas se encuentran actualizados a versiones sin vulnerabilidades críticas. SO.1-2: Se tienen identificados aquellos activos que por su tecnología no pueden ser actualizados, detallando los controles compensatorios implementados. Nivel 2: SO.1-3: Está definido un plan documentado para la gestión de las vulnerabilidades y parches. SO.1-4: Se reciben notificaciones de vulnerabilidades por parte del CERTuy u otras organizaciones y se analizan.

	SO.1-5: Las vulnerabilidades son evaluadas, clasificadas, y priorizadas según la criticidad identificada. Nivel 3: SO.1-6: Existe un procedimiento documentado de gestión de vulnerabilidades y parches. SO.1-7: Están establecidas las responsabilidades de gestión de vulnerabilidades. SO.1-8: Los escaneos de vulnerabilidades se realizan como mínimo semestralmente. Nivel 4: SO.1-9: Se realizan revisiones de control interno sobre el plan de gestión de vulnerabilidades. SO.1-10: El resultado de las revisiones se comunica al RSI. SO.1-11: Se documentan las lecciones aprendidas, que aportan a la mejora de futuras resoluciones frente a vulnerabilidades similares.
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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	Las herramientas usadas en el análisis de vulnerabilidades deben estar homologadas o ser recomendadas por instituciones de prestigio internacional.
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

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.
Controles	Nivel 1: SO.2-1: Se han establecido mecanismos para comunicar los cambios en el ámbito tecnológico a las partes interesadas. SO.2-2: Los cambios tecnológicos son previamente autorizados por los responsables de los activos. Nivel 2: SO.2-3: Se definen el versionado, las líneas base de configuración y los lineamientos de hardenizado de los productos de software. SO.2-4: Los cambios de configuración sobre infraestructura crítica requieren validación previa mediante pruebas en ambientes controlados. Nivel 3:

	SO.2-5: Está definida una política de gestión de cambios, la misma contempla los cambios de emergencia en el ámbito tecnológico. SO.2-6: Está establecido y documentado un procedimiento para la gestión de los cambios. SO.2-7: Los cambios se registran y se les asocia una justificación y responsable. Nivel 4: SO.2-8: Se cuenta con herramientas para dar soporte a la gestión de los cambios. SO.2-9: Se realizan actividades de control interno para revisar el cumplimiento de los procedimientos relacionados a gestión de cambios. SO.2-10: El resultado de estas actividades es comunicado al RSI y demás partes interesadas. SO.2-11: Se toman medidas correctivas ante desvíos.
Guía de implementación	**Alcance de la gestión de los cambios** 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. **Política de gestión de cambios** La política de gestión de cambios debe 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. **Procedimiento de gestión de cambios** 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. **Puertos de diagnóstico y configuración remota** Los puertos, servicios y aplicaciones instalados en un equipos o sistemas de red, que no sean específicamente necesarios para las operaciones del negocio, se desactivan o eliminan. El acceso a puertos de diagnóstico y configuración se controla mediante cerraduras y procedimientos que restringen su uso a personal autorizado.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	Los procedimientos, sistemas y hardware se encuentran actualizados, conforme las necesidades del negocio.
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. • Procedimientos de hardenización de servidores. • Procedimiento de control de acceso con medidas específicas para puertos de diagnóstico y configuración remota. • Informes de revisión periódica del proceso de gestión de cambios.
Normativa asociada	N/A

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.
Controles	Nivel 1: SO.3-1: La capacidad actual instalada es suficiente para garantizar la prestación de los servicios críticos. SO.3-2: Ante eventos de saturación o cuellos de botella se toman medidas ad-hoc para restaurar la capacidad operativa.

	Nivel 2: SO.3-3: Se toman en cuenta las necesidades del negocio al momento de dimensionar los servicios críticos. SO.3-4: Se realizan mediciones objetivas para detectar problemas de capacidad. Nivel 3: SO.3-5: Está establecido el proceso de gestión de la capacidad. SO.3-6: Los roles y responsabilidades asociados al proceso de gestión de la capacidad están definidos y documentados. SO.3-7: La gestión de capacidad se integra en los acuerdos de nivel de servicio vigentes. Nivel 4: SO.3-8: Existe un plan de capacidad formalizado y documentado. SO.3-9: Está definido un proceso de estimación de la capacidad que acompaña al plan. SO.3-10: Se revisa periódicamente el plan de capacidad. SO.3-11: Se proponen acciones para la mejora continua de la gestión de la capacidad.
Guía de implementación	**Alcance de la gestión de la capacidad** 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. **Identificación de los requisitos de capacidad** 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 deberá poder realizar mediciones objetivas para detectar problemas de capacidad. **Plan de gestión de la capacidad** 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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Reportes o alertas de saturación, picos de uso, degradación de servicio o fallas atribuible • Análisis de tendencias y proyecciones de crecimiento documentadas. • Registros de revisión del plan de capacidad y acciones tomadas a partir de dichos análisis. • Evidencia de uso del plan de capacidad como insumo para planificación de proyectos, presupuestos, compras.
Normativa 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.
Controles	Nivel 1:

	SO.4-1: El entorno de producción se encuentra separado del resto de los entornos. Nivel 2: SO.4-2: Se cuenta con plataformas adecuadas e independientes que soportan el ciclo de vida de desarrollo de los sistemas. SO.4-3: Se implementan controles para el pasaje entre los ambientes. SO.4-4: Se evita el uso de datos reales de producción en ambientes de prueba; en caso de ser necesarios, se aplican controles de acceso adecuados al nivel de confidencialidad de la información. Nivel 3: SO.4-5: Se encuentra definida una política de separación de entornos. SO.4-6: Está establecido y documentado un procedimiento de gestión de ambientes. SO.4-7: Están definidos los responsables para la gestión de los ambientes existentes y de los pasajes a producción. SO.4-8: Durante la realización de las pruebas se registra y conserva la información del entorno (características, información de los datos de prueba, etc.). Nivel 4: SO.4-9: Se realizan auditorías de cumplimiento y control interno de la política de separación de entornos y procedimientos relacionados. SO.4-10: Se registran los resultados y se toman acciones correctivas en casos de desvíos.
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 deberá 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).
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	Existen procedimientos para verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas Se tienen procedimientos y controles para el paso de programas a producción.
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.

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).
Controles	Nivel 1: SO.5-1: Todos los equipos del personal cuentan con solución antimalware. SO.5-2: Las soluciones a los problemas detectados se realizan en forma ad-hoc. Nivel 2: SO.5-3: Los servidores cuentan con una solución antimalware, salvo excepciones justificadas. SO.5-4: Se encuentran configurados chequeos periódicos en los equipos del personal. Nivel 3: SO.5-5: Está definida una política del manejo de software malicioso.

	SO.5-6: Está establecido un procedimiento del manejo de software malicioso. SO.5-7: Se cuenta con una solución centralizada de antimalware. Nivel 4: SO.5-8: Están implementados controles para evitar el acceso a sitios Web maliciosos y/o no autorizados. SO.5-9: La protección ante software malicioso se extiende a otros dispositivos móviles y se refleja en la política de protección contra software malicioso. SO.5-10: Existen procedimientos documentados para la detección de equipos que se encuentran desprotegidos y se realizan las acciones necesarias para subsanar la situación. SO.5-11: Se cuenta con un registro estadístico de infecciones por software malicioso que aporta a la toma de decisiones y alimenta las lecciones aprendidas que se usan para la mejora continua.
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 antimalware centralizada y su responsable para la gestión. ● Capacitar al personal afectado en la operación y uso de la solución antimalware, 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 protección** Se debe contar con herramientas automatizadas (EDR, XDR, antispyware, firewalls personales, IPS, etc.), de preferencia centralizadas, para monitorear continuamente estaciones de trabajo, servidores y dispositivos móviles. **Protección contra software malicioso en servidores** Se debe implementar una estrategia de defensa en profundidad que combine múltiples capas de seguridad interconectadas. El núcleo de esta estrategia es la adopción de una solución avanzada de

	Detección y Respuesta Extendidas (XDR), que integra y correlaciona datos de diversas fuentes más allá del endpoint. Esta plataforma XDR debe incorporar las capacidades de una solución de protección de endpoints (EPP/EDR). Simultáneamente, es fundamental reducir la superficie de ataque mediante el hardening del sistema operativo. La estrategia debe reforzarse con sistemas de detección y prevención de intrusiones (IDS/IPS) y monitoreo. Aquellos servidores que, debido a limitaciones tecnológicas inherentes, no puedan alojar un agente de protección, deberán ser monitoreados de forma compensatoria, justificando claramente el motivo de la excepción y las medidas alternativas aplicadas.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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 antimalware actualizado. • Cantidad de licencias vs cantidad de equipos de la organización. • 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

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.
Controles	Nivel 1: SO.6-1: Se realizan respaldos periódicos de al menos los activos de información del centro de procesamiento de datos (aplicaciones, bases de datos, máquinas virtuales, etc.). Nivel 2:

	SO.6-2: Los respaldos se almacenan en lugares seguros y con acceso restringido. SO.6-3: Se establece el grado (completo, diferencial, etc.) y los requisitos de retención de los respaldos. SO.6-4: Los respaldos son probados regularmente. SO.6-5: Los respaldos se almacenan en medios inmutables o fuera de línea, para evitar posibles compromisos de ransomware. Nivel 3: SO.6-6: Se cuenta con soluciones automatizadas para asistir en la realización de los respaldos. SO.6-7: Existe una política de respaldos. SO.6-8: Existen procedimientos documentados de realización y prueba de recuperación de respaldos. Nivel 4: SO.6-9: El procedimiento de respaldos se actualiza ante cambios de requerimientos del negocio o cambios de infraestructura o sistemas que requieran acciones de respaldo. SO.6-10: La política y el procedimiento de respaldo se encuentran alineados al plan de contingencia y al plan de recuperación. SO.6-11: La política y procedimiento de respaldos se revisan regularmente.
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. **Protección de datos personales** 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 con 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 63/023 de la URCDP indica cuáles son los países adecuados: miembros de la Unión Europea y el Espacio Económico Europeo, Principado de Andorra, República Argentina, el sector privado de Canadá, Guernsey, Isla de Man, Islas Feroe, Estado de Israel, Japón, Jersey, Nueva Zelanda, Reino Unido de Gran Bretaña e Irlanda del Norte, y Confederación Suiza. Se declaran también como adecuadas las transferencias realizadas por entidades sujetas a la Ley de Protección de la Información Personal de la República de Corea, y las transferencias a organizaciones incluidas en el "Listado del Marco de Privacidad de Datos" publicado por el Departamento de Comercio de los estados Unidos de América. 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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	Se cuenta con procedimientos y mecanismos de retención de datos conforme a lo estipulado por la normativa vigente.
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 - Resoluciones 63/023 y 70/023 URCDP - Dictamen 08/2014 de fecha 23/7/2014 Otras que puedan establecer períodos de retención y otros requisitos asociados.

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.
Controles	Nivel 1: SO.7-1: Están configurados los registros de auditoría y eventos para todos los sistemas definidos como críticos. SO.7-2: Se analiza el impacto de los eventos que afectan a los sistemas y servicios más críticos, dentro o fuera del centro de procesamiento de datos. SO.7-3: Existe personal con tareas asignadas para la detección de eventos a nivel de sistemas base y de protección perimetral. Nivel 2: SO.7-4: Se cuenta con herramientas para la centralización de logs. SO.7-5: Los registros están protegidos contra accesos no autorizados y posibles alteraciones. SO.7-6: Se establecen los umbrales tolerables de los activos (por ejemplo, tiempo de espera tolerable para una aplicación Web). SO.7-7: Los sistemas que soportan los servicios críticos emiten alertas de eventos de forma independiente, basados en las pautas establecidas por el apetito de riesgo de la organización. SO.7-8: Se automatizan alertas ante eventos de seguridad de la información. Por ejemplo, permiten alertar cuando los usuarios realizan conexiones fuera de la organización, y la conexión e instalación de dispositivos o software no autorizado en equipos de la organización. SO.7-9: Se han definido las responsabilidades y la participación de los roles de TI en las actividades de monitoreo, incluyendo aquellas basadas en herramientas automatizadas. SO.7-10: Se establecen los requisitos de retención de los registros de auditoría.

	SO.7-11: Los relojes de todos los sistemas deben estar sincronizados (servidores, aplicaciones, etc.) Nivel 3: SO.7-12: Se tiene en cuenta los requisitos de confidencialidad de la información y protección de la privacidad de los datos contenidos en los registros. SO.7-13: Se define una política de auditoría y registro de eventos, como por ej. de los sistemas y redes y de configuración y uso de WAF. SO.7-14: Están establecidos procedimientos de auditoría y registro de eventos. SO.7-15: Se cuenta con herramientas que permitan la correlación de eventos de seguridad de la información. SO.7-16: Están establecidos procedimientos de detección y monitoreo. SO.7-17: Las actividades de identificación de impacto y determinación de umbrales están contenidas en el procedimiento de detección y monitoreo. SO.7-18: Se realizan pruebas periódicas al procedimiento de monitoreo. SO.7-19: Se cuenta con mecanismos para revisar las actividades de los administradores. Nivel 4: SO.7-20: Se cuenta con herramientas que permitan respuesta automatizada ante incidentes de seguridad de la información. SO.7-21: Se realizan actividades de control interno para verificar el cumplimiento con la política y los procedimientos. SO.7-22: El resultado de las revisiones se comunica al RSI y demás partes interesadas.
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 deberá 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. **Registro de eventos de sistemas y usuarios**

	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 deben 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 debe 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 deben centralizarse para facilitar su revisión y estar protegidos contra accesos no autorizados. Se debe 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. **Revisiones periódicas de los registros** Se debe establecer un procedimiento de revisión periódica de los registros generados y definir los responsables de la realización y periodicidad de las revisiones. **Sincronización de relojes** 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.
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.”
Instituciones Emisoras de Dinero Electrónico (IEDE)	Se tiene un procedimiento establecido para registrar, controlar, rastrear y restringir el acceso a los datos de pago sensibles. Se cuenta con mecanismos automatizados para aislar los activos de información afectados en caso de ciberataques, con el fin de minimizar y prevenir el contagio, especialmente en los procesos financieros interconectados.
Guía de evidencia para auditoría	● Política de auditoría 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

Requisito SO.8	Gestionar la instalación de software.
Objetivo	Garantizar la integridad y seguridad de los sistemas.
Controles	Nivel 1: SO.8-1: Están definidas las pautas para la instalación de software. SO.8-2: Las pautas de instalación de software fueron difundidas al personal. Nivel 2: SO.8-3: La posibilidad de instalar software en los equipos queda restringida a los usuarios que se encuentran autorizados para ese fin. SO.8-4: Se asegura una estricta segregación entre las utilidades del sistema y el software de aplicaciones, limitando el acceso a las utilidades del sistema. Nivel 3: SO.8-5: Existen listas de software autorizados, las que son revisadas y aprobadas por el RSI. Nivel 4: SO.8-6: Se realizan actividades de control interno sobre el software instalado con el fin de determinar el cumplimiento de la lista de software autorizado. SO.8-7: Los resultados de estas revisiones son enviados al RSI y demás partes interesadas.
Guía de implementación	**Procedimientos de instalación de software** 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. **Gestión de licencias de software** 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. **Control de herramientas administrativas** Se debe asegurar una estricta segregación entre las herramientas administrativas del sistema y el software de aplicaciones, limitando el acceso a las herramientas administrativas del sistema únicamente a usuarios autorizados y que lo requieran para cumplimiento de sus funciones.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Listado de herramientas administrativas del sistema y usuarios autorizados a su uso. • Requerimientos a nivel legal y normativo para la instalación y uso de las licencias de software.
Normativa asociada	N/A

2.8 Seguridad de las comunicaciones

Requisito SC.6	Establecer acuerdos de no divulgación.
Objetivo	Proteger la información de la organización.

Controles	Nivel 1: SC.6-1: Los nuevos proveedores de servicios deben firmar acuerdos de confidencialidad o no divulgación (NDA) antes del inicio de la relación contractual. SC.6-2: Todo nuevo personal incorporado debe estar cubierto por cláusulas confidencialidad y no divulgación, ya sea en acuerdos, estatuto o normativa interna. Nivel 2: SC.6-3: La obligación de confidencialidad y no divulgación se extiende a todo el personal de la organización, independientemente de su rol o tipo de contratación. SC.6-4: Todos los proveedores que deban acceder a información confidencial de la organización deben tener firmado un acuerdo de no divulgación. Nivel 3: SC.6-5: Se detallan en los acuerdos de no divulgación las responsabilidades y sanciones por incumplimiento. Nivel 4: SC.6-6: Se revisan los acuerdos de no divulgación de forma periódica para verificar pertinencia en relación a los objetivos de negocio. SC.6-7: El resultado de las revisiones se comunica al RSI y demás partes interesadas.
Guía de implementación	**Protección de datos** 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. **Definición de acuerdos de no divulgación** 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. **Revisión de los acuerdos** Los acuerdos deben revisarse periódicamente y cuando surgen cambios que influyan en los requisitos anteriormente mencionados. En particular, dentro de la administración pública, los funcionarios públicos tienen contemplada esta obligación dentro de la ley 19.823, no

	obstante, el resto de los colaboradores con otras relaciones contractuales deberán firmar algún acuerdo de no divulgación que podrá estar reflejado (típicamente) en un acuerdo como tal, o en cláusulas de confidencialidad (u otras) dentro del contrato.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	Los empleados y subcontratados que hayan tenido conocimiento y acceso a datos reservados deberán suscribir acuerdos de confidencialidad.
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. Ley 19.823: Declaración de interés general del código de ética en la función pública

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.
Controles	Nivel 1: SC.12-1: El servicio de Webmail de la organización se implementa exclusivamente sobre el protocolo HTTPS. SC.12-2: El acceso al Webmail institucional está restringido únicamente al servicio provisto por la organización, prohibiendo el acceso a cuentas institucionales desde Webmail externos. SC.12-3: Los certificados digitales utilizados para el servicio de Webmail son válidos, vigentes y emitidos por una Autoridad Certificadora de confianza. Nivel 2: SC.12-4: Las configuraciones del servicio de Webmail bloquean el uso de protocolos inseguros o versiones obsoletas de TLS/SSL. SC.12-5: Se revisan periódicamente los registros de acceso para verificar que no existan conexiones desde servicios de Webmail externos no autorizados.

	SC.12-6: Se generan alertas ante intentos de acceso no autorizados al Webmail. Nivel 3: SC.12-7: Cuando corresponda según la clasificación de la información transmitida vía email, se utiliza cifrado a nivel de mensaje (por ejemplo, S/MIME o PGP, etc). SC.12-8: Los titulares de cuentas institucionales reciben instrucciones y capacitación sobre el uso seguro del Webmail y la prohibición de acceso desde servicios externos. Nivel 4: SC.12-9: Se realizan auditorías periódicas para verificar el cumplimiento de las restricciones de acceso y la vigencia de los certificados digitales. SC.12-10: Se realizan pruebas técnicas para validar el cifrado de las comunicaciones y la correcta configuración de seguridad del servicio de Webmail.
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. 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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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	Ley 18.331: Protección de datos personales y habeas data

Requisito SC.13	Debe existir segregación a nivel de servicios de información.
Objetivo	Asegurar la capacidad para gestionar de manera segura los servicios de red y definir acuerdos de interconexión formalmente autorizados.
Controles	Nivel 1: SC.13-1: La red se encuentra segmentada al menos en redes con contacto directo con redes externas (por ejemplo, Internet) y redes privadas de la organización. SC.13-2: Están identificados y documentados los principales servicios de red utilizados por la organización. SC.13-3: Se mantiene un inventario actualizado de las interconexiones con otras entidades. Nivel 2: SC.13-4: Se segmenta la red en función de las necesidades de la organización. SC.13-5: Se genera una postura de manejo de tráfico por defecto entre segmentos. SC.13-6: Las conexiones con otras entidades están formalmente autorizadas mediante acuerdos de seguridad de interconexión que describen interfaz, requisitos de seguridad y datos intercambiados. SC.13-7: Los proveedores de servicios de red cuentan con acuerdos de nivel de servicio (SLA) y cláusulas de seguridad. Nivel 3: SC.13-8: Esta definida una política formal de seguridad de las comunicaciones. SC.13-9: Se cuenta con un diagrama de red actualizado que refleja la segregación vigente y las interconexiones externas.

	SC.13-10: Se conoce y se analiza el tráfico en los diferentes segmentos de la red. SC.13-11: Las comunicaciones entrantes y salientes entre los diferentes segmentos son protegidas. Nivel 4: SC.13-12: Se cuenta con un proceso de control interno que verifica el cumplimiento de la segregación definida y de los acuerdos de interconexión. SC.13-13: Se revisan periódicamente los SLA, contratos y condiciones técnicas de los proveedores de red y conectividad.
Guía de implementación	**Política de seguridad de las comunicaciones** Definir una política de seguridad de las comunicaciones donde se contemplen al menos los siguientes puntos: ● Objetivos y alcance de las comunicaciones (internas/externas, remotas e inalámbricas). ● Requisitos mínimos para protección del canal (p. ej., TLS/HTTPS, SSH, IPsec) y autenticación. ● Criterios para interconexiones externas (deben estar autorizadas y sujetas a acuerdos de seguridad). ● Lineamientos para gestión de incidentes de comunicaciones y conservación de registros (logs). ● Roles y responsabilidades (quién aprueba interconexiones, quién opera, quién revisa). **Diagrama de red** Se debe contar con diagrama/s de red actualizado/s. **Autorización y control de interconexiones** Formalizar cada conexión externa mediante un acuerdo de seguridad de interconexión que detalle: propósito, datos, cifrado/autenticación, filtrado, puntos de terminación, responsabilidades operativas y de incidentes, y contactos. Mantener inventario y expiraciones/renovaciones. **Protecciones entre segmentos** Implementar filtrado de tráfico en perímetros internos y externos, inspección de estado, listas de control por dirección/puerto/aplicación, y—cuando aplique—proxying y egress filtering. Documentar reglas, cambios y responsables. **Relación con proveedores** Incluir en los contratos con proveedores SLAs y cláusulas de seguridad (soporte, tiempos de atención, gestión de incidentes, pruebas de conectividad, ventanas de mantenimiento, auditoría razonable). Realizar revisiones periódicas y conservar evidencias.

	Para el intercambio seguro de información entre organismos Agesic disponibiliza la Plataforma de Interoperabilidad (PDI) de la Plataforma de Gobierno Electrónico (PGE).
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Política de seguridad de las comunicaciones • Procedimiento para la segregación de las redes • Diagrama de red detallado indicando la segregación definida (en caso de existir) • Inventario de servicios de red e interconexiones con metadatos y registro de autorizaciones formales que incluyan los requisitos de cada conexión • Rol o función de administrador de seguridad con descripción de tareas • Personal asignado a la administración de la red, monitoreo y revisión • Lista de proveedores de servicios de red • Acuerdos de seguridad de interconexión y sus renovaciones • Contratos y SLA de proveedores con registro de revisiones periódicas • Registro de auditorías efectuadas a proveedores • Registro de revisiones periódicas de contratos y SLA (si no se incluye directamente en el ítem de contratos)
Normativa 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
Controles	Nivel 1: SC.14-1: Se implementan controles criptográficos para proteger los datos en tránsito. Nivel 2: SC.14-2: Los datos en tránsito de todas las aplicaciones y sistemas se encuentran protegidos mediante un mismo conjunto reducido de tecnologías y prácticas criptográficas. Nivel 3:

	SC.14-3: La organización cuenta con procedimientos documentados para la transferencia segura de información física y digital. SC.14-4: Los procedimientos para la transferencia de información establecen medidas de seguridad diferenciadas según el nivel de sensibilidad de los datos involucrados. SC.14-5: Se realizan acuerdos formales con terceras partes que establecen responsabilidades y medidas de seguridad para la transferencia de información. Nivel 4: SC.14-6: Se realizan revisiones periódicas sobre los controles criptográficos utilizados para asegurar la protección de los datos que son enviados y recibidos por los diferentes sistemas y aplicaciones.
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 debe 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. **Acuerdos de transferencia segura** A nivel de lo que es 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”.
Instituciones de salud	-

Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Acuerdos o cláusulas contractuales con terceros que incluyan medidas de seguridad para la transferencia segura de datos. • Evidencia de revisiones periódicas sobre el uso de controles criptográficos.
Normativa asociada	

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.
Controles	Nivel 1: SC.15-1: Existe un inventario de sitios Web institucionales. SC.15-2: Todas las aplicaciones Web disponibles en Internet se encuentran protegidas mediante el uso de WAF, al menos configurados en modo “detección”. Nivel 2: SC.15-3: El WAF de producción ha evolucionado de modo detección a modo bloqueo. Nivel 3: SC.15-4: Se cuenta con un WAF instalado en ambiente de prueba para la realización de pruebas funcionales. SC.15-5: En el ambiente de producción se impactan las reglas actualizadas luego de ser probadas. SC.15-6: Los registros de los WAF se encuentran centralizados. Nivel 4: SC.15-7: El análisis de los registros del WAF incluye automatismos que favorecen las actividades de revisión.
Guía de implementación	Instalar un WAF delante del sitio Web (por ejemplo, el módulo de Apache mod_security, F5, Coraza, 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 los momentos iniciales, luego de su instalación, se recomienda dejarlo en modo “escucha” para aprender del tráfico y poder ajustar el WAF a las necesidades del sitio Web; para luego pasarlo a modo “bloqueo”. En producción siempre debe estar en modo “bloqueo” para que éste cumpla su objetivo.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Configuración de WAF. • Reportes realizados al CERTuy o equipo de respuesta correspondiente. • Inventario de los sitios web institucionales, incluyendo el nivel de protección configurado en los WAF.
Normativa asociada	N/A

2.9 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 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.
Controles	Nivel 1: AD.1-1: Se cuenta con lineamientos generales para el desarrollo de los sistemas incluyendo principios básicos de la gestión de proyectos. Nivel 2: AD.1-2: Se incorporan principios de desarrollo seguro en los proyectos de desarrollo de sistemas. AD.1-3: Se cuenta con mecanismos para el control de versiones y revisión de código. AD.1-4: Se sistematizan las actividades de prueba, incluyendo casos de prueba orientados a las validaciones de seguridad. Nivel 3: AD.1-5: Se define un procedimiento documentado de pruebas de seguridad. AD.1-6: Se definen los criterios de aceptación de los productos desde la perspectiva de seguridad de la información. AD.1-7: Los desarrollos subcontratados deben cumplir con requisitos mínimos de seguridad establecidos por la organización,

	independientemente del ciclo de desarrollo utilizado por el proveedor. Nivel 4: AD.1-8: Se realizan actividades de control interno para determinar el nivel de cumplimiento con la metodología y procedimientos definidos. AD.1-9: El resultado de estas actividades se comunica al RSI y demás partes interesadas. AD.1-10: Se toman acciones correctivas frente a desvíos detectados en los proyectos de desarrollo o adquisición.
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 debe ser fácil de mantener y legible.

	Control de versiones Se debe contar con mecanismos para el control de versiones y revisión de código, como Git, Subversion, SourceSafe, CVS, ClearCase, entre otros, con el objetivo de restringir el acceso al código fuente y a las bibliotecas relacionadas. Esto previene añadir o modificar contenido sin autorización. El acceso queda limitado exclusivamente a individuos autorizados, asegurando que solo aquellos con necesidades laborales legítimas puedan realizar cambios o consultas. Se establecen reglas específicas para el acceso, con una supervisión detallada de las actualizaciones y accesos al código por parte de los usuarios. **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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	Los sistemas informáticos de la institución deben contar con soporte por parte del fabricante o proveedor autorizado por este. En caso contrario deberá justificarse y establecerse controles paliativos. Las interfases de los sistemas de cara al público (clientes) establecen y cumplen con criterios de seguridad y calidad (por ejemplo, OWASP ASVS, usabilidad, etc.)
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. • Documentación de pruebas de seguridad, criterios de aceptación y entregables vinculados a requisitos de seguridad.

	• Evidencias de versionado de archivos y control de acceso al repositorio de código fuente.
Normativa asociada	N/A

Requisito AD.2	Incluir requisitos de seguridad de la información para la adquisición de productos y servicios de tecnología.
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.
Controles	Nivel 1: AD.2-1: Se cuenta con lineamientos generales para la adquisición de sistemas o servicios de tecnología. AD.2-2: Los requisitos de seguridad de la información se incluyen en las solicitudes y evaluaciones de compra. Nivel 2: AD.2-3: Se evalúa la capacidad de los proveedores para cumplir con los requisitos de seguridad antes de la contratación. Nivel 3: AD.2-4: Se revisan y aprueban los entregables para verificar que cumplen con los requisitos de seguridad definidos. AD.2-5: Los contratos con proveedores incluyen compromisos de mantenimiento de la seguridad a lo largo del ciclo de vida del producto o servicio. Nivel 4: AD.2-6: Los procesos de adquisición consideran las lecciones aprendidas y resultados de auditorías para mejorar continuamente los requisitos de seguridad.
Guía de implementación	**Adquisición de productos** 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. **Definición de requisitos y evaluación previa** Antes de iniciar un proceso de compra, la organización debe definir los requisitos de seguridad específicos basados en un análisis de riesgos. Estos pueden incluir, entre otros: autenticación y control de acceso, cifrado de datos, registro de eventos, cumplimiento normativo, gestión de vulnerabilidades y soporte de actualizaciones de seguridad. Se debe evaluar la capacidad del proveedor para cumplir con dichos requisitos y considerar el historial de cumplimiento de seguridad. **Incorporación de requisitos en los contratos**

	Los contratos y acuerdos con los proveedores deben contener cláusulas que establezcan obligaciones claras en materia de seguridad de la información, protección de datos, gestión de incidentes y mantenimiento de actualizaciones de seguridad durante la vida útil del producto o servicio, entre otras. En caso de que no sea posible cumplir con un requisito crítico, se debe documentar el riesgo y someterlo a aprobación para su aceptación formal. **Seguimiento y verificación** Una vez adquirido el producto o servicio, se deben establecer mecanismos de verificación que permitan confirmar que los entregables cumplen con los requisitos de seguridad. Esto puede incluir pruebas técnicas, revisiones documentales y validaciones operativas. Adicionalmente, se debe realizar un seguimiento periódico del proveedor para evaluar el cumplimiento continuo de los compromisos asumidos en materia de seguridad.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	Los sistemas informáticos de la institución deben contar con soporte por parte del fabricante o proveedor autorizado por este. En caso contrario deberá justificarse y establecerse controles paliativos.
Guía de evidencia para auditoría	• Lineamientos generales aprobados para la adquisición de sistemas o servicios de tecnología (políticas internas, resoluciones, etc.). • Solicitudes de compra o pliegos de licitación que incluyan requisitos de seguridad de la información. • Actas o informes de revisión y aprobación de entregables, evidenciando la verificación de requisitos de seguridad definidos.
Normativa asociada	

2.10 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.
Controles	Nivel 1: RP.1-1: Se identifican todos los participantes de la cadena de suministro relacionados con los activos y servicios críticos, incluyendo un punto de contacto operativo designado por cada proveedor. RP.1-2: Se cuenta con acuerdos de nivel de servicio (SLA) firmados con proveedores que prestan servicios críticos.

	Nivel 2: RP.1-3: Se implementan mecanismos para identificar y gestionar los riesgos asociados a los participantes de la cadena de suministro que intervienen en los activos y servicios críticos de la organización. RP.1-4: Los contratos con proveedores críticos deben incluir cláusulas que obliguen a notificar de forma oportuna cualquier incidente de seguridad, confirmado o sospechado, que pueda afectar a la organización. RP.1-5: Los contratos deben establecer claramente la responsabilidad del proveedor en la protección de la información de la organización y en la implementación de las medidas de respuesta acordadas. Nivel 3: RP.1-6: Se cuenta con una política formal de relacionamiento con proveedores. RP.1-7: Está definido un procedimiento documentado de gestión de proveedores que abarca la selección, contratación, seguimiento, y finalización del vínculo. Nivel 4: RP.1-8: Se aplica la gestión de riesgos en la adquisición de productos y servicios, y se mantiene en todo el ciclo de vida de los mismos.
Guía de implementación	**Soporte, mantenimiento y régimen de cobertura** Todo sistema, servicio y equipamiento crítico del centro de procesamiento 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 procesamiento de datos requiere atención en modalidad 7x24 (o la que mejor se adapte a las necesidades del negocio). **Acuerdos de nivel de servicio** Muchas veces las organizaciones no tienen la capacidad operativa para cubrir este servicio por lo que delegan o comparten la operación del centro de procesamiento 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 procesamiento de datos. **Tiempos de respuesta** 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.

	Transferencia de responsabilidades Los acuerdos deben especificar la transferencia de responsabilidades legales y de cumplimiento, incluyendo la protección de los datos personales y la propiedad intelectual. Es crucial establecer mecanismos para ajustar estos acuerdos ante cambios en los requisitos o el fin de la relación, asegurando una terminación ordenada y la continuidad operativa. **Reporte de incidentes** Debe definirse un procedimiento para el reporte de incidentes confirmados o sospechados por parte de los proveedores. Los proveedores deben estar obligados a notificar a la organización sobre cualquier incidente confirmado o sospechado tras su descubrimiento, garantizando que dicha notificación se realice sin demoras irrazonables y, respetando los plazos legales. Esta notificación debe incluir la identificación de todos los individuos cuya información personal haya sido comprometida.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Listado de proveedores de servicios críticos. • Política de relacionamiento con proveedores. • Procedimiento de gestión de proveedores. • Procedimiento de reporte de incidentes de seguridad de la información (el mismo debe incluir la forma de reporte de proveedores). • Contrato con proveedores y acuerdos de nivel de servicio (SLA). Que incluyan cláusulas de seguridad de la información. • 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	

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.
Controles	Nivel 1:

	RP.2-1: Se definen métricas e indicadores para el seguimiento y control de los proveedores, mínimamente para los proveedores críticos. Nivel 2: RP.2-2: Los contratos y acuerdos con proveedores críticos incluyen cláusulas que permiten su revisión o ajuste en caso de cambios en los servicios prestados, en las tecnologías utilizadas o en las normativas aplicables. Nivel 3: RP.2-3: Se define la periodicidad de las evaluaciones de los proveedores. RP.2-4: Se documentan los resultados de las evaluaciones de desempeño y cumplimiento de requisitos de seguridad de los proveedores. RP.2-5: Se registra y mantiene evidencia de los incumplimientos contractuales o desviaciones detectadas en los servicios provistos, incluyendo las acciones tomadas ante los mismos. Nivel 4: RP.2-6: Se revisan periódicamente los acuerdos con proveedores críticos para asegurar su adecuación a los requerimientos actuales del negocio y a cambios regulatorios. RP.2-7: La gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio. RP.2-8: Las evaluaciones son tomadas en cuenta para las actualizaciones de contratos y las futuras adquisiciones.
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.
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.
Instituciones Emisoras de Dinero Electrónico (IEDES)	Existe personal responsable para el seguimiento de los acuerdos contractuales celebrados con proveedores terceros de servicios de tecnología. Se mantendrá y actualizará un registro de información en relación con todos los acuerdos contractuales sobre el uso de servicios de tecnología prestados por proveedores relevantes y otros terceros. Se definen criterios para seleccionar proveedores de servicios de computación en la nube.

	Se verifica que los proveedores de servicios de computación en la nube cuenten y mantengan vigente las certificaciones adecuadas. Se implementan mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los proveedores y terceros, incluyendo proveedores de servicio de computación en nube.
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

2.11 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.
Controles	Nivel 1: GI.1-1: Se encuentran identificados los puntos de contacto inicial para la recepción de eventos de seguridad. Nivel 2: GI.1-2: Se identifican los potenciales actores internos y externos ante un incidente y se registran sus datos de contacto. GI.1-3: Se cuenta con herramientas que apoyan la gestión de los incidentes. Nivel 3: GI.1-4: Se ha definido un procedimiento general que cubre las distintas fases de gestión de incidentes (detección, registro, análisis, contención, erradicación y cierre). GI.1-5: Se encuentra definida formalmente la política de gestión de incidentes de seguridad de la información. GI.1-6: La política de gestión de incidentes es difundida a todas las partes interesadas. Nivel 4: GI.1-7: Se realizan auditorías internas para verificar el cumplimiento con la política y procedimientos relacionados. GI.1-8: El resultado de estas actividades se informa al RSI y se toman acciones correctivas frente a desvíos y para la mejora continua.
Guía de implementación	**Política de gestión de incidentes** Se debe definir una política de gestión de incidentes de seguridad de la información. **Responsables de la gestión de incidentes** Asimismo, se deben definir las responsabilidades para la gestión de los incidentes de seguridad de la información de la organización y del personal. **Procedimientos de gestión de incidentes** 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). **Mejora continua** 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. Las entidades vinculadas a servicios críticos deberán 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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Auditorías internas realizadas sobre el proceso de gestión de incidentes.
Normativa asociada	

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	Identificar el impacto y alcance de un evento de seguridad y determinar si requiere ser tratado como un incidente.
Controles	Nivel 1: GI.2-1: Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas. GI.2-2: Se han definido lineamientos para la categorización de los incidentes según su tipo y criticidad. Nivel 2: GI.2-3: Está definido cuando una serie de eventos o una notificación conforman un incidente. GI.2-4: Está definido cuando una serie de eventos o una notificación conforman un delito conforme la normativa vigente. GI.2-5: Los incidentes identificados se clasifican utilizando una escala formal de severidad y criticidad.

	GI.2-6: Están definidas las acciones y tiempos de respuesta asociados a cada categoría según severidad. Nivel 3: GI.2-7: Existe un procedimiento de gestión de incidentes que incluye las tareas de análisis de impacto. GI.2-8: El procedimiento de gestión de incidentes define el criterio para escalar un incidente considerando: activos afectados, criticidad y severidad. GI.2-9: Se cuenta con herramientas automatizadas para el registro de incidentes alineadas con el plan y/o procedimiento de respuesta definido. GI.2:10: Las acciones asociadas a cada categoría están alineadas al plan de respuesta. Nivel 4: GI.2-11: La categorización de incidentes se revisa periódicamente, considerando las necesidades del negocio y las tendencias de amenazas. GI.2-12: Se realizan estadísticas utilizando las categorizaciones. GI.2-13: Los resultados son utilizados para mejorar o incrementar los controles existentes.
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 debe 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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Estadísticas generadas sobre incidentes.
Normativa asociada	Ley 20327 normas para la prevención y represión de la ciberdelincuencia

Requisito GI.3	Informar de forma completa e inmediata a las partes interesadas.
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. Asimismo, identificar si se debe reportar a otras partes interesadas como organismos reguladores, propietarios de datos, clientes, u entidades, conforme lo establezca la normativa vigente o las políticas internas de la organización.
Controles	Nivel 1: GI.3-1: Los incidentes de seguridad informática se reportan al CERTuy y/o al equipo de respuesta que corresponda de acuerdo a los criterios establecidos por éste. GI.3-2: Los incidentes de seguridad que involucre datos personales son reportados a la Unidad Reguladora y de Control de Datos Personales (URCDP), conforme a los plazos y requisitos establecidos por la normativa vigente. GI.3-3: Los incidentes de seguridad que pueda corresponder a un delito son denunciados ante la Unidad de cibercrimen. Nivel 2: GI.3-4: Se lleva un registro de las comunicaciones realizadas ante incidentes, incluyendo hora, contenido y destinatarios. Nivel 3: GI.3-5: Se ha documentado un procedimiento formal de comunicación de incidentes. Nivel 4: GI.3-6: El procedimiento de comunicación de incidentes se revisa regularmente y se ajusta ante cambios regulatorios, lecciones aprendidas o recomendaciones del CERTuy. GI.3-7: Se realizan simulacros de reporte de incidentes para validar la efectividad del canal de comunicación y los tiempos de reacción. GI.3-8: Se auditan periódicamente los canales, mecanismos y procedimientos de notificación establecidos para incidentes de seguridad.
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.

	Siempre debe contactarse al CERTuy por las vías de comunicación publicadas en su sitio Web: www.cert.uy. Las entidades obligadas deben comunicar la ocurrencia de incidentes de ciberseguridad al CERTuy en un plazo de 24 (veinticuatro) horas de conocido el incidente, según lo establecido en el artículo 10 del decreto 66/025. **Unidad de cibercrimen (Ministerio del interior - Policía Nacional).** Si se identifica un incidente que pueda corresponder a un delito, se debe presentar una denuncia ante la Unidad de cibercrimen para iniciar la investigación judicial correspondiente. Datos de contacto de la Unidad de Cibercrimen (Dirección de Investigaciones de la Policía Nacional) • Dirección: Carlos Quijano 1316, Montevideo • Correo electrónico: dipn-cibercrimen@minterior.gub.uy Tel: 2030-4625 Quien realice la denuncia penal debe tener poder de representación del organismo. **Unidad de Regulación y Control de Datos Personales (URCDP).** Si se sospecha o confirma que los datos personales están afectados, el incidente debe reportarse a la URCDP dentro de las 72 horas, según lo establecido en el artículo 4 del decreto 64/020. Acceda a la información sobre el proceso de reclamo ante la URCDP .
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”.
Instituciones Emisoras de Dinero Electrónico (IEDE)	Sí un incidente de seguridad afectará o pudiera afectar a los intereses financieros de los usuarios de sus servicios de pago, el proveedor de servicios de pago les informará. Se le debe notificar al BCU conforme la normativa vigente.
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. • Registro de comunicaciones realizadas ante incidentes durante el período auditado. • Registro o actas de simulacros de notificación de incidentes. • Auditorías internas o revisiones periódicas realizadas sobre los canales, mecanismos y procedimientos de comunicación definidos.

Normativa asociada	Ley 20.327 Decreto 64/020 Decreto 66/025

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.
Controles	Nivel 1: GI.4-1: Los incidentes de seguridad se reportan internamente de acuerdo a lineamientos preestablecidos. GI.4-2: El personal ha sido instruido sobre los mecanismos y canales habilitados para reportar incidentes. GI.4-3: Los incidentes son registrados. Nivel 2: GI.4-4: Los registros de incidentes permiten trazabilidad completa de su evolución, desde la detección hasta el cierre. Nivel 3: GI.4-5: Existe un procedimiento de registro que incluye campos como: fecha/hora, tipo de incidente, activos afectados, estado, entre otros campos relevantes. GI.4-6: El reporte de incidentes se apoya en herramientas automatizadas. Nivel 4: GI.4-7: Se realizan actividades de control interno de cumplimiento con el procedimiento de reporte de incidentes. GI.4-8: El resultado de las actividades se utiliza para mejorar el procedimiento de reporte.
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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-

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. • Documentación que evidencie la evolución del incidente desde la detección hasta el cierre.
Normativa asociada	

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
Controles	Nivel 1: GI.5-1: Se han definido los mecanismos de respuesta a incidentes. GI.5-2: Los incidentes son atendidos y se aplican medidas para mitigar sus consecuencias. Nivel 2: GI.5.3: Ante un incidente de seguridad de la información en la organización, se realiza un análisis forense. GI.5-4: Se han definido pautas establecidas para garantizar la cadena de custodia. GI.5-5: Se han definido pautas para contener el daño y minimizar el riesgo en el entorno operativo. GI.5-6: Se cuenta con planes de remediación de los incidentes. Nivel 3: GI.5-7: Está definido un plan y/o procedimiento de respuesta ante incidentes. GI.5-8: Todos los procedimientos vinculados al análisis forense se encuentran documentados. GI.5-9: Se define el responsable de la respuesta a incidentes. GI.5-10: Se cuenta con pautas o políticas documentadas para llevar adelante las revisiones de las estrategias de respuesta. GI.5-11: Se revisan periódicamente las estrategias de respuesta de los procesos de la organización que afecten los servicios críticos. GI.5-12: Los incidentes de severidad alta son reportados mediante informe a la Dirección u otras partes interesadas. Nivel 4: GI.5-13: El plan de respuesta a incidentes es probado anualmente. GI.5-14: La Dirección, el RSI y el CSI reciben información periódica sobre incidentes de seguridad de la información. GI.5-15: Se realizan auditorías internas para verificar el cumplimiento del plan y/o procedimiento de respuesta. GI.5-16: Las mejoras identificadas en las revisiones de estrategia son utilizadas para su ajuste. GI.5-17: Se generan indicadores para seguimiento y control.

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 debe 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. **Registro de las actividades de respuesta** 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. **Informe de incidentes**

	Los informes de incidentes deberán tener como mínimo un resumen objetivo de los acontecimientos, indicando la severidad y taxonomía del incidente. Se deberá evaluar en cada caso la pertinencia de hacer la reserva de dicho informe, bajo las pautas establecidas de la ley 18.381 de acceso a la información pública.
Instituciones de salud	El plan de gestión de incidentes debe contemplar el equipamiento médico.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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	Ley 18.381 acceso a la información pública

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.
Controles	Nivel 1: GI.6-1: Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en el centro de procesamiento de datos. Nivel 2: GI.6-2: Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en toda la organización. Nivel 3: GI.6-3: Las lecciones aprendidas son puestas a disposición y comunicadas a todas las partes interesadas. GI.6-4: Se cuenta con herramientas que dan soporte al registro y gestión de las lecciones aprendidas. GI.6-5: Las lecciones aprendidas se contemplan para mejorar los planes de respuesta a incidentes. GI.6-6: Las lecciones aprendidas son utilizadas para mejorar los canales de comunicación establecidos con las partes involucradas y los procesos de escalamiento. Nivel 4:

	GI.6-7: Las lecciones aprendidas son utilizadas para la mejora de los procesos de la organización. GI.6-8: Se generan indicadores para seguimiento y control. GI.6-9: Se definen indicadores para poder medir la efectividad de los controles.
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. • 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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Informe de evaluación de daños. • Informe de lecciones aprendidas. • Repositorio de lecciones aprendidas. • Evidencia de comunicación interna de lecciones aprendidas. • Evidencia de que los planes fueron ajustados con base en lo aprendido de incidentes anteriores. • Indicadores definidos para medir efectividad de controles. • Documentación de uso de una herramienta o sistema para el registro y gestión de lecciones aprendidas.
Normativa asociada	

2.12 Continuidad de las operaciones

Requisito CO.1	Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de procesamiento de datos.
Objetivo	Garantizar el normal funcionamiento de los centros de procesamiento de datos y operaciones.
Controles	Nivel 1: CO.1-1: El centro de procesamiento de datos cuenta con UPS y componentes redundantes en lo que refiere a conexión eléctrica. CO.1-2: El centro de procesamiento de datos cuenta con componentes redundantes de acondicionamiento térmico. Nivel 2: CO.1-3: El centro de procesamiento de datos cuenta con generador eléctrico capaz de alimentar a todos los componentes críticos. CO.1-4: Los sistemas de climatización del centro de procesamiento de datos están alimentados por líneas de energía respaldadas por el generador eléctrico. Nivel 3: CO.1-5: El sistema de climatización está configurado para operar de forma continua 24/7 y contempla mecanismos automáticos de failover ante fallas. CO.1-6: Se realizan pruebas periódicas de funcionamiento de los mecanismos automáticos de failover en los sistemas de climatización. Nivel 4: CO.1-7: Se realizan pruebas periódicas de funcionamiento del generador y UPS para validar su operatividad ante fallas reales. CO.1-8: Se realizan revisiones periódicas del diseño de redundancia del centro procesamiento de datos considerando cambios tecnológicos, de carga o de riesgos identificados. CO.1-9: La organización cuenta con un sitio de contingencia capaz de asegurar la continuidad operativa en caso de indisponibilidad del centro de procesamiento de datos principal, incluyendo pruebas periódicas de su capacidad y tiempo de conmutación.
Guía de implementación	Para la implementación de controles de acceso físico a los centros de procesamiento de datos y áreas relacionadas. **Suministro de energía** ● Se debe contar con un sistema generador de energía eléctrica con capacidad suficiente para abastecer todo el centro de procesamiento 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 procesamiento 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 procesamiento 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 procesamiento 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 procesamiento 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 procesamiento de datos durante estos cortes. Actualmente casi todos los activos de un centro de procesamiento 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 procesamiento 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. **Climatización** ● 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 procesamiento 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. En los casos donde el centro de procesamiento de datos sea en la nube, todos los controles deberán estar cubiertos por el proveedor, debiendo presentar certificaciones o constancias que avalen esto.
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 procesamiento de datos.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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	

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 procesamiento de datos no tenga puntos únicos de falla, es decir, que la operativa del centro de procesamiento de datos pueda continuar aun ante la caída de un activo de red.
Controles	Nivel 1: CO.2-1: El centro de procesamiento de datos cuenta con componentes redundantes en lo que refiere a infraestructura de comunicaciones. Nivel 2: CO.2-2: La organización dispone de conectividad a internet a través de múltiples enlaces o proveedores. CO.2-3: Los equipos de red críticos del centro de procesamiento de datos están configurados con mecanismos de detección automática de fallos. Nivel 3: CO.2-4: La arquitectura de red del centro de procesamiento de datos, incluyendo su esquema de redundancia, está documentada y actualizada.

	CO.2-5: Se realizan pruebas periódicas de conmutación automática de enlaces o equipos de red redundantes, y se registran sus resultados. Nivel 4: CO.2-6: La organización realiza revisiones técnicas periódicas del diseño de la red para identificar nuevos puntos únicos de falla y definir mejoras. CO.2-7: Se analizan eventos o fallos reales en la infraestructura de red para ajustar la estrategia de redundancia y disponibilidad.
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. En los casos donde el centro de procesamiento de datos sea en la nube, todos los controles deberán estar cubiertos por el proveedor, debiendo presentar certificaciones o constancias que avalen esto.
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 procesamiento de datos.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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. • Documento de arquitectura de red del centro de procesamiento de datos, incluyendo su esquema de redundancia.
Normativa asociada	

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 servicios críticos.

Controles	Nivel 1: CO.4-1: Se cuenta con ciertas medidas de contingencia y recuperación para los sistemas que dan soporte a los servicios críticos. CO.4-2: Están identificados un conjunto de amenazas que podrían afectar la continuidad operativa. CO.4-3: Existen respaldos de información de los sistemas que dan soporte a los servicios críticos. Nivel 2: CO.4-4: Existen planes formales de contingencia operativa y de recuperación ante desastres, validados por la alta dirección. CO.4-5: Se ha identificado el orden de prelación para la recuperación en base a la dependencia de los servicios. Nivel 3: CO.4-6: Se cuenta con un Análisis de Impacto al Negocio (BIA) que identifica los procesos críticos. CO.4-7: Se ejecutan pruebas puntuales o parciales de los planes. Nivel 4: CO.4-8: Se ha definido el o los responsables del mantenimiento de los planes de contingencia y de recuperación. CO.4-9: Los planes de contingencia y de recuperación contemplan la participación de proveedores de servicios críticos, acorde a los acuerdos de nivel de servicio (SLA) y su involucramiento en las pruebas de contingencia. CO.4-10: Se registran los resultados de las pruebas. CO.4-11: El resultado de las pruebas retroalimenta las lecciones aprendidas y sirven para la mejora continua de los planes y procedimientos.
Guía de implementación	**Planificación, Políticas y procedimientos** 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.

	Metodología para la planificación de la continuidad operativa Para cumplir con estas premisas, la organización debe 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. **Plan de contingencia y recuperación** Una vez analizados los aspectos anteriormente mencionados, la organización debe confeccionar formalmente un plan de contingencia y recuperación. **Pruebas al plan de contingencia y recuperación** Se debe establecer también un plan de pruebas al plan de contingencia y recuperación, con una frecuencia al menos anual. Para optimizar estas pruebas, se debe identificar el orden de prelación para la recuperación en base a la dependencia de los servicios. Se debe tener en cuenta la incorporación de los proveedores de servicios críticos para la realización del plan y pruebas de contingencia y recuperación. **Capacitación al personal** Se debe también planificar la capacitación del personal con relación a la continuidad operativa. **Comunicación** Se debe 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.
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. Considerar en el plan de continuidad operativa, cuando el personal de TI y médico comparten instalaciones, los planes de prevención y mitigación del contagio del personal de TI ante el caso de aparición de una enfermedad altamente contagiosa.

Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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	

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.
Controles	Nivel 1: CO.5-1: Está designado un responsable o equipo para la identificación de métricas de recuperación para procesos críticos. Nivel 2: CO.5-2: Se han definido formalmente las ventanas de tiempo máximo soportadas por el negocio sin poder operar (MTD), para cada sistema que soporte un proceso crítico. CO.5-3: Se ha determinado el RTO (Recovery Time Objective) para cada sistema que soporte un proceso crítico. CO.5-4: Se ha definido el RPO (Recovery Point Objective) para cada sistema que soporte un proceso crítico. Nivel 3: CO.5-5: Las métricas MTD, RTO y RPO han sido utilizadas para identificar brechas entre los tiempos actualmente alcanzables y los requerimientos definidos. CO.5-6: Las métricas definidas han sido incorporadas como insumo obligatorio en el diseño, pruebas y evaluación de los planes de continuidad. CO.5-7: Las métricas son revisadas periódicamente y actualizadas ante cambios en procesos o tecnologías. Nivel 4: CO.5-8: Los resultados de las pruebas de continuidad son comparados contra las métricas definidas y se documentan desviaciones con planes de mejora asociados. CO.5-9: Las métricas son utilizadas como insumo en análisis costo-beneficio para priorizar inversiones en infraestructura, redundancia o automatización de recuperación.
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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	● Plan de continuidad de las operaciones. ● Plan de recuperación ante desastres.
Normativa asociada	

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.
Controles	Nivel 1: CO.6-1: La comunicación externa de las situaciones de crisis o incidentes mayores es llevada a cabo exclusivamente por la Dirección o por quien ésta haya determinado. CO.6-2: Las áreas técnicas pueden realizar comunicaciones externas sólo si cuentan con autorización expresa de la Dirección o por quien ésta haya determinado. Nivel 2: CO.6-3: Se ha comunicado quién es el vocero designado y a través de qué canales debe ser contactado. Nivel 3: CO.6-4: Se ha definido y documentado un plan y/o procedimiento de comunicaciones ante crisis que cubre la evaluación del evento, las notificaciones, nivel de comunicación requerido, mensajes, audiencia, interesados y monitoreo de las comunicaciones. CO.6-5: El plan y/o el procedimiento han sido difundidos entre todos los actores involucrados en la gestión de crisis y continuidad operativa. Nivel 4: CO.6-6: Se realizan ensayos periódicos que incluyen la ejecución del plan y procedimiento de comunicación ante crisis, de forma coordinada con los ejercicios de continuidad y recuperación.

	CO.6-7: Se realizan auditorías internas para verificar el cumplimiento del plan y procedimiento de comunicaciones ante crisis. CO.6-8: Los resultados de las revisiones y ensayos son documentados y utilizados para ajustar, actualizar y mejorar continuamente el plan y procedimiento de comunicaciones. CO.6-9: La Dirección participa activamente en las actualizaciones del plan, en especial, en la aprobación y modo de difusión de los mensajes.
Guía de implementación	**Plan de comunicaciones** 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. **Pruebas al plan de comunicaciones** El plan de comunicaciones debe probarse periódicamente en escenarios en conjunto con el plan de contingencia y recuperación. **Equipo de comunicaciones** La definición del equipo de comunicaciones debe figurar o referenciarse en el plan de contingencia y recuperación.

Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Plan de contingencia y recuperación. • Plan de comunicaciones ante crisis.
Normativa asociada	N/A

2.13 Cumplimiento normativo y revisión

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.
Controles	Nivel 1: CN.1-1: Se identifican los requisitos normativos relacionados a seguridad de la información y ciberseguridad, protección de datos personales, acceso a la información pública, propiedad intelectual, y otras obligaciones legales, contractuales o políticas que resulten exigibles para la organización. Nivel 2: CN.1-2: El delegado de protección de datos personales trabaja de manera coordinada con el RSI y/o CSI. Nivel 3: CN.1-3: Se han definido procedimientos para incorporar nuevos requisitos legales o normativos cuando sean publicados. CN.1-4: El resultado es comunicado al RSI y/o al CSI. Nivel 4: CN.1-5: Se realizan auditorías internas para verificar el cumplimiento. CN.1-6: Los resultados de las revisiones se utilizan para la mejora continua y apoyan a la toma de decisiones.
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.
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.
Instituciones Emisoras de Dinero Electrónico (IEDE)	Colaborar con los entes reguladores, en los proyectos futuros sobre seguridad de la información con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.
Guía de evidencia para auditoría	• Resolución u otro mecanismo o registros que evidencie formalmente la adopción de la política de seguridad de la información. • Registro de base de datos (Protección de datos, Derecho de acceso a la información pública). • Listado de legislación aplicable a la organización. • Informes de auditoría sobre el cumplimiento normativo de la organización
Normativa asociada	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.)

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.
Controles	Nivel 1: CN.2-1: Se han realizado análisis de brechas para detectar el nivel de cumplimiento del presente marco. CN.2-2: En función de las brechas detectadas se elabora un portafolio de proyectos a incluir en el plan de seguridad de la información. Nivel 2: CN.2-3: Se realiza anualmente una auditoría interna sobre el cumplimiento del presente marco. Nivel 3: CN.2-4: Se realiza con una periodicidad predefinida una auditoría externa sobre el cumplimiento del presente marco. CN.2-5: Los hallazgos de auditorías generan planes de acción documentados y se realiza su seguimiento. Nivel 4: CN.2-6: Se evalúa periódicamente la calidad y alcance de las auditorías realizadas, incorporando lecciones aprendidas para futuras ejecuciones. CN.2-7: Las auditorías incluyen en su alcance la revisión completa del sistema de gestión de seguridad de la información y sus objetivos, políticas y controles definidos.
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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Análisis de brecha de seguridad de la información. • Plan de seguridad de la información. • 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

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.
Controles	Nivel 1: CN.3-1: Se realizan revisiones puntuales de los sistemas de información con recursos propios o con apoyo externo. Nivel 2: CN.3-2: Se realizan pruebas de intrusión (ethical hacking) de los sistemas críticos de la organización en forma periódica o como parte de un cambio significativo en ellos, con recursos propios o con apoyo externo. CN.3-3: El resultado de las pruebas se comunica a las partes interesadas. Nivel 3: CN.3-4: Está establecido un procedimiento documentado para la revisión periódica interna de vulnerabilidades con alcance a los sistemas base y de aplicación. CN.3-5: En los sistemas críticos se realizan los escaneos de vulnerabilidades con un periodo entre ellos de máximo 6 meses

	y pruebas de intrusión con un periodo entre ellas de máximo un año. CN.3-6: Se cuenta con el apoyo de revisiones externas de vulnerabilidades y hackeo ético. Nivel 4: CN.3-7: Los resultados de las revisiones internas y externas se utilizan para la mejora continua de la seguridad de los sistemas. CN.3-8: Se realizan actividades de control interno para verificar el cumplimiento con el procedimiento de revisión periódica de vulnerabilidades. CN.3-9: El procedimiento de revisión de vulnerabilidades se encuentra incorporado en las actividades de seguridad de la información.
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.
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. En el de caso de productos cerrados, se debe exigir al proveedor la presentación del informe con resultados de la ejecución del EH, junto con la evidencia de la resolución de los hallazgos o análisis de riesgo correspondiente.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Evidencia de la realización de pruebas de intrusión. • Plan de acción para las acciones correctivas.
Normativa 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.

Controles	Nivel 1: CN.4-1: Se lleva control del licenciamiento de software de equipos servidores. Nivel 2: CN.4-2: Se han definido responsables para la gestión del ciclo de vida del licenciamiento, incluyendo adquisición, asignación, renovación y baja. CN.4-3: Se lleva control del licenciamiento de software de equipos personales. Nivel 3: CN.4-4: El inventario centralizado de software instalado en la organización debe permitir asociar licencias activas con las instalaciones detectadas. Nivel 4: CN.4-5: Se realiza una revisión periódica del uso real de licencias adquiridas para detectar sobrelicenciamiento o subutilización. CN.4-6: Se realizan análisis periódicos del cumplimiento de los términos y condiciones de uso de las licencias adquiridas.
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.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
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

2.14 Protección de datos personales

Requisito PD.1	Principio de Legalidad
Objetivo	Asegurar que el tratamiento de datos personales se realice conforme a la Ley 18.331 (Protección de datos personales y habeas data).
Controles	Nivel 1:

	PD.1-1: Se lleva un inventario actualizado de bases de datos personales, incluyendo responsables, categoría de datos y sistemas que las soportan. PD.1-2: Todas las bases de datos que contienen datos personales están registradas ante la URCDP. Nivel 2: PD.1-3: Se cuenta con un estudio de la normativa vigente que debe cumplir cada base de datos registrada. Nivel 3: PD.1-4: Se realizan revisiones periódicas del cumplimiento legal del tratamiento de datos personales en los sistemas y procesos de la organización. PD.1-5: Se implementan medidas correctivas cuando se detectan incumplimientos en materia de legalidad del tratamiento de datos. Nivel 4: PD.1-6: Se ha integrado la revisión del cumplimiento legal del tratamiento de datos personales dentro del proceso de auditoría interna.
Guía de implementación	Las bases de datos que contengan datos personales deben cumplir con la normativa vigente y estar inscriptas en el registro correspondiente, el cual está a cargo de la Unidad Reguladora y de Control de Datos Personales (URCDP)
Instituciones de salud	La ley de protección de datos personales establece como datos sensibles aquellos datos que abarcan aspectos esenciales del individuo, como su salud, características físicas, ideología, y vida sexual, entre otros, requiriendo consentimiento expreso y escrito para su tratamiento. Además, la ley también indica que la recolección de datos relativos a la salud debe realizarse por establecimientos sanitarios públicos o privados y por profesionales vinculados a las ciencias de la salud física o mental de los pacientes que acuden a ellos, o que estén o hubieran estado bajo tratamiento en aquellos. La historia clínica incluye datos sensibles, detallando, entre otros: enfermedades, tratamientos, adicciones (si las tiene), información genética, y potencialmente datos sobre raza, sexualidad o creencias religiosas. Estos datos son cruciales para la asistencia sanitaria, asegurando que médicos y centros dispongan de la información necesaria para una atención adecuada. El centro de salud debe mantener una historia clínica detallada, ya sea en formato papel o electrónico, que registre la trayectoria de salud del individuo desde su nacimiento hasta su fallecimiento. Además, el tratamiento de este tipo de datos sensibles requiere el consentimiento expreso y escrito de los titulares de los datos. Esto implica que, si un usuario cambia de institución o de sistema de cobertura de salud, para obtener la historia clínica completa de la

	institución de origen, es necesario contar con dicho consentimiento, basándose en la normativa vigente. Asimismo, esta ley establece que únicamente las instituciones autorizadas para tratar datos sensibles pueden crear bases de datos con este tipo de contenido. Sin perjuicio de la normativa en materia de salud que permite el traspaso de historias clínicas de un prestador a otro.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Listado de bases de datos con datos personales. • Evidencia del registro de las bases de datos personales, con la debida resolución de inscripción a la URCDP. • Evidencia de los consentimientos de comunicación de datos personales sensibles. • Listado de sistemas que dan soporte a las bases de datos personales.
Normativa asociada	• Ley 18.331: Protección de datos personales y habeas data • Normativa complementaria y concordante.

Requisito PD.2	Principio de Veracidad
Objetivo	Garantizar que los datos personales recolectados estén actualizados, sean veraces, adecuados, ecuánimes y relevantes para la finalidad.
Controles	Nivel 1: PD.2-1: Se cuenta con mecanismos para recibir solicitudes expresas de los titulares de corrección manual de datos personales. PD.2-2: La organización establece qué datos personales son necesarios para cada trámite o servicio, y limita su recolección únicamente a esa información. Nivel 2: PD.2-3: Se lleva un registro documentado de todas las solicitudes recibidas por parte de los titulares de datos personales, relativas a la actualización, eliminación o rectificación de sus datos, incluyendo el plazo en que cada solicitud fue atendida. PD.2-4: Cuando el titular de los datos personales se encuentra presente, se procede a validar la exactitud de los datos y, en caso de corresponder, se actualizan los datos en los sistemas correspondientes en ese mismo momento. Nivel 3: PD.2-5: Los sistemas implementan funcionalidades que requieren a los usuarios la revisión y validación periódica de sus datos personales, con el objetivo de identificar y corregir información inexacta o desactualizada. PD.2-6: Los sistemas que gestionan datos personales registran las modificaciones realizadas, incluyendo la fecha del cambio y la identidad del usuario que lo efectuó.

Guía de implementación	La organización debe garantizar que la recopilación de datos personales se limite estrictamente a la información relevante y necesaria para su fin. Es fundamental que los datos recolectados sean siempre veraces, pertinentes, ecuánimes (imparciales) y proporcionados en relación con la finalidad de su obtención. Un claro ejemplo de recolección excesiva sería la solicitud de preferencias políticas para la afiliación a un club deportivo. La normativa establece que, al detectarse la inexactitud o falsedad de los datos personales, el responsable debe proceder a suprimirlos, sustituirlos o completarlos según corresponda a cada caso. Para ello, es esencial realizar revisiones en los sistemas o programas relevantes, con el fin de identificar y actualizar cualquier dato personal que resulte inexacto o desactualizado, manteniendo así el compromiso con el principio de veracidad de los datos personales. A modo de ejemplo, en el caso de que una persona desee actualizar su estado civil en una base de datos privada tras un cambio, debe presentar prueba fehaciente de este cambio y el responsable de la base debe proceder con la actualización de la información correspondiente. Se deberán tener registradas las actualizaciones realizadas en la información, para en caso de tener que recurrir a un respaldo de información, poder reaplicar el cambio en caso de requerirse.
Instituciones de salud	Con la excepción de situaciones de emergencia, los datos deberán recabarse directamente del usuario para garantizar su veracidad. El paciente tiene derecho a estar informado sobre los nombres, cargos y roles de todos los trabajadores de la salud involucrados en su cuidado. La institución debe publicar la nómina de los profesionales activos en el ámbito de la salud, incluyendo sus nombres, especialidades y cualquier otro dato relevante, junto con sus días y horarios de consulta.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Listado de bases de datos con datos personales. • Listado de sistemas que dan soporte a las bases de datos personales. • Evidencia de análisis de la necesidad de la recolección de los datos personales para el fin y/o fundamento legal de la información tratada. • Evidencia de verificación y/o actualización de datos personales.
Normativa asociada	• Ley 18.331: Protección de datos personales y habeas data. • Ley 18.335: Derechos y obligaciones de pacientes y usuarios de los servicios de salud. • Normativa complementaria y concordante.

Requisito PD.3	Principio de Finalidad
Objetivo	Definir, comunicar y documentar claramente los propósitos del tratamiento de datos.
Controles	Nivel 1: PD.3-1: Se han eliminado de forma ad-hoc datos personales que ya no eran necesarios para el fin con el que fueron recolectados. PD.3-2: Se documenta la finalidad del tratamiento de datos personales en todos los procesos que los recolectan. Nivel 2: PD.3-3: Se han establecido criterios sobre cuánto tiempo se conservarán los datos personales en función de su finalidad. PD.3-4: Se mantienen registros de las eliminaciones o anonimizaciones de datos personales, acorde al procedimiento. Nivel 3: PD.3-5: Se han implementado procedimientos para eliminar o anonimizar los datos personales una vez cumplida su finalidad. PD.3-6: Se revisan periódicamente las bases de datos con el objetivo de identificar datos cuya finalidad ya se ha cumplido. Nivel 4: PD.3-7: La revisión del cumplimiento de la finalidad del tratamiento de los datos personales ha sido incorporada como parte del alcance del proceso de auditoría interna.
Guía de implementación	Los datos personales solo deben emplearse para los fines específicos por los cuales se recopilaron. Una vez alcanzado el propósito inicial, estos datos deben ser eliminados. Por ejemplo, tras la realización de un sorteo, se deben suprimir los datos personales recabados para dicho evento. También se pueden mantener cuando puedan existir obligaciones legales, pero en ese caso los datos deben permanecer bloqueados. Por ej. casos de responsabilidad contractual o extracontractual. Vencidos esos plazos si corresponde o la eliminación o realizar el procedimiento de conservación. Sin embargo, este mismo principio contempla excepciones en las que, por motivos históricos, estadísticos o científicos y de acuerdo con la legislación aplicable, es posible conservar los datos personales incluso cuando no exista una necesidad o pertinencia directa. El artículo 37 del decreto N° 414/009 detalla el procedimiento para solicitar la autorización de esta conservación de datos, basándose en las finalidades mencionadas, y requiere que el responsable de los datos presente una petición fundamentada para obtener dicha autorización. En este caso la organización debe analizar la factibilidad y pertinencia de utilizar técnicas para proteger los datos, como por ej.: minimización de datos, seudonimización o anonimización.

Instituciones de salud	● La historia clínica del paciente se mantiene durante la vida del paciente y después las instituciones médicas las pueden conservar (bloqueadas) mientras existen obligaciones legales. ● Los datos de sistemas de apoyo a la historia clínica, como por ejemplo los PACs, deben ser retenidos por el período de tiempo que se estime necesario según las políticas y obligaciones legales de la organización. Una vez culminado este período las mismas deberán ser eliminadas. ● Los datos de auditoría de los sistemas de historia clínica deben ser retenidos por un período de tiempo que se estime necesario según las políticas de la organización. Una vez culminado este período las mismas deberán ser eliminadas.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	Evidencia de procesos y procedimientos de eliminación de datos personales una vez que cumplieron su cometido.
Normativa asociada	● Ley 18.331: Protección de datos personales y habeas data ● Artículo 37° del decreto N°414/009 ● Normativa complementaria y concordante.

Requisito PD.4	Principio de previo consentimiento informado
Objetivo	Asegurar que los individuos tengan pleno conocimiento y comprensión de cómo se tratarán sus datos personales antes de que otorguen su consentimiento previo e informado.
Controles	Nivel 1: PD.4-1: Cuando corresponde, se incluye una cláusula de consentimiento libre, previa e informada en los medios utilizados para recabar los datos personales (formularios, grabaciones, sitios web, etc.). PD.4-2: Se conservan registros que evidencien el consentimiento otorgado por los titulares, siempre que sea exigido por la normativa. Nivel 2: PD.4-3: Se verifica, previo al tratamiento de datos personales, si el consentimiento del titular es requerido según lo establecido por la normativa vigente. PD.4-4: Los mecanismos que requieren consentimiento informado garantizan que la opción de aceptar o rechazar esté claramente visible y no preseleccionada. PD.4-5: Cuando el tratamiento se basa en el consentimiento, se han definido mecanismos que permiten a los titulares revocar el consentimiento otorgado en cualquier momento, sin afectar la licitud del tratamiento previo. Nivel 3: PD.4-6: Existen procedimientos documentados que establecen cómo identificar los casos en los que se requiere consentimiento, y cómo obtener, registrar y conservarlo de manera adecuada.

	PD.4-7: Los mecanismos para ejercer la revocación del consentimiento están disponibles públicamente y son fácilmente accesibles. Nivel 4: PD.4-8: Se ha incorporado la verificación del consentimiento informado como parte de las auditorías internas periódicas. PD.4-9: Se revisan y actualizan periódicamente los textos, formularios y canales utilizados para recabar el consentimiento informado.
Guía de implementación	La organización debe solicitar y registrar de manera libre, previa e informada el consentimiento del titular para tratar sus datos, pudiendo recabar dicho consentimiento a través de distintas formas como grabaciones, formularios o aceptación en sitios web, dependiendo del tipo de dato o mecanismo de comunicación. Sin embargo, existen ciertas excepciones a la regla del previo consentimiento informado. Estas incluyen: los datos que provienen de fuentes públicas de información, como registros o publicaciones en medios masivos, definidos taxativamente en el artículo 9° bis de la Ley 18331; los datos recabados para funciones estatales o bajo obligación legal; y los datos incluidos en listados que, para personas físicas, se limitan a nombres, apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, y para personas jurídicas, incluyen razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo. Además, se consideran excepciones los datos derivados de relaciones contractuales, científicas o profesionales necesarios para su desarrollo, así como aquellos recabados por individuos para uso personal, individual o doméstico. Cabe destacar que, aunque la información del Diario Oficial, registros públicos y publicaciones en medios de comunicación son considerados fuentes públicas, Internet en su conjunto no califica como tal. Es importante tener en cuenta los artículos 5° y 6° del decreto N°414/009, que estipulan requisitos especiales para la recolección del consentimiento. El artículo 5° especifica que se debe informar a los titulares de los datos personales sobre la finalidad específica del tratamiento de sus datos y el tipo de actividad que realiza el responsable de la base de datos o tratamiento. El incumplimiento de esta obligación de informar adecuadamente invalida el consentimiento obtenido. Por último, el artículo 6° detalla las formas adecuadas para recabar el consentimiento, estableciendo que el deber de obtenerlo se considera cumplido cuando se ofrece al titular la elección entre dos opciones claramente identificadas, las cuales no deben estar

	premarcadas a favor o en contra, garantizando así una elección auténticamente libre e informada.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	● Procesos y procedimientos de obtención de consentimientos informados por base de datos. ● Listado de consentimientos informados obtenidos por base de datos.
Normativa asociada	● Ley 18.331: Protección de datos personales y habeas data ● Artículos 5° y 6° del decreto N°414/009 ● Normativa complementaria y concordante.

Requisito PD.5	Principio de seguridad de los datos
Objetivo	Definir las medidas que deben adoptar los responsables o usuarios de bases de datos para garantizar la seguridad y la confidencialidad de los datos personales.
Controles	Nivel 1: PD.5-1: Se han restringido los accesos a los datos personales mediante usuarios nominados y aplicando el principio de mínimo privilegio. PD.5-2: Se han implementado medidas para restringir el acceso no autorizado a documentos físicos que contienen datos personales. Nivel 2: PD.5-3: Se implementan medidas técnicas y organizativas necesarias para preservar la integridad, confidencialidad y disponibilidad de la información, garantizando así la seguridad de los datos personales. PD.5-4: Se mantiene un registro de incidentes de seguridad que involucren datos personales, incluyendo la fecha y tipo de evento. Nivel 3: PD.5-5: Se mantienen registros que permiten auditar el acceso a datos personales sensibles. Dichos registros permiten identificar quién accedió, en qué momento y a qué tipo de información. PD.5-6: Existen procedimientos para notificar incidentes de seguridad a la URCDP dentro del plazo legal establecido, incluyendo la evaluación del impacto y acciones tomadas. PD.5-7: Está definido un procedimiento formal para comunicar a los titulares de datos las vulneraciones de seguridad. Nivel 4: PD.5-8: Se realizan simulaciones para verificar la eficacia de las medidas de seguridad aplicadas a los datos personales, incluyendo escenarios de incidentes o accesos indebidos.

	PD.5-9: La Dirección revisa periódicamente el tratamiento de los riesgos sobre datos personales y aprueba medidas estratégicas para reforzar su protección.
Guía de implementación	La organización debe implementar medidas orientadas a proteger los datos personales contra cualquier forma de adulteración, pérdida, acceso o tratamiento no autorizado. Esto incluye la detección de cualquier desviación de la información, ya sea intencional o accidental, originada por acciones humanas o fallos en los sistemas técnicos. De acuerdo con el artículo 3 del decreto N°64/020, tanto el responsable como el encargado del tratamiento de datos deben adoptar las medidas técnicas y organizativas necesarias para preservar la integridad, confidencialidad y disponibilidad de la información, garantizando así la seguridad de los datos personales. Se recomienda considerar la adopción de estándares nacionales (como el presente Marco de Ciberseguridad) o internacionales de seguridad de la información. En caso de incidentes de seguridad que resulten en la divulgación, destrucción, pérdida o alteración de datos personales, o el acceso no autorizado a estos, se deben iniciar procedimientos para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de haber sido constatados. El artículo 4 establece que, tras constatar una vulneración de seguridad que afecte la protección de datos, el responsable del tratamiento debe notificarla a la Unidad Reguladora y de Control de Datos Personales (URCDP) en un plazo máximo de 72 horas. Esta comunicación debe incluir detalles relevantes como la fecha de la vulneración, su naturaleza, los datos personales afectados y los posibles impactos. Además, si la vulneración afecta significativamente los derechos de los titulares de los datos, debe comunicarse a estos en un lenguaje claro y sencillo. Una vez resuelta la vulneración, se debe elaborar y comunicar un informe detallado de la incidencia y las medidas adoptadas a la URCDP. Los datos deben ser almacenados de manera que se permitan el ejercicio del derecho de acceso por parte de sus titulares, asegurando así su capacidad para revisar, modificar o eliminar su información personal conforme a la ley. Además, se prohíbe el registro de datos personales en bases de datos que no cumplan con las condiciones técnicas mínimas de integridad y seguridad. Esto implica la implementación de controles robustos (técnicos, personales y procesos) que protejan contra la manipulación indebida, el acceso no autorizado y otros riesgos potenciales, garantizando la confidencialidad, integridad y disponibilidad de la información. Las medidas pueden ser físicas, como, por ejemplo, utilizar llaves de seguridad, alarmas, control de ingreso, y también

	medidas lógicas, como por ejemplo usuarios nominados, contraseñas seguras y monitoreo, entre otras.
Instituciones de salud	Los centros de salud están obligados a implementar medidas de seguridad para las historias clínicas, ya sea que estén en formato papel o electrónico. Los centros de salud deben desarrollar políticas y procedimientos de seguridad de la información, designando además a un responsable para su gestión. Además, durante la transferencia de información o traslado de documentos, se deben adoptar todas las medidas necesarias para preservar su confidencialidad e integridad. De igual manera, cualquier proceso de destrucción de información debe asegurar que los datos no puedan ser recuperados posteriormente. Estos criterios de seguridad también deben aplicarse cuando el tratamiento de los datos esté a cargo de terceros en representación del centro asistencial, lo cual se debe gestionar aplicando las normativas específicas Ley 18.335 y decreto 274/010.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	● Medidas técnicas implementadas por cada base de datos. ● Registro de incidentes de seguridad que involucren datos personales, junto a sus fechas ciertas de detección, atención, reporte a la URCDP y reporte a los afectados. ● Procesos y procedimientos que permiten a los titulares hacer ejercicio de sus derechos. ● Matrices de control de acceso a los datos personales para las bases involucradas.
Normativa asociada	● Ley 18.331: Protección de datos personales y habeas data ● Artículos 3° y 4° del decreto N°64/020 ● Ley 18.335: Derechos y obligaciones de pacientes y usuarios de servicios de salud ● Decreto 274/010. ● Normativa complementaria y concordante.

Requisito PD.6	Principio de reserva
Objetivo	Asegurar que los datos personales sean utilizados en forma reservada y utilizarse únicamente para el tratamiento habitual de su actividad.
Controles	Nivel 1: PD.6-1: El acceso a datos personales está limitado únicamente a las personas que realizan tareas directamente asociadas con la finalidad específica para la cual dichos datos fueron recabados. Nivel 2:

	PD.6-2: Están definidos y documentados los roles autorizados a acceder a datos personales y las finalidades permitidas para su uso. PD.6-3: Los contratos, reglamentos o políticas internas contemplan sanciones explícitas ante el uso o divulgación indebida de datos personales. PD.6-4: El personal autorizado a tratar datos personales está sujeto a compromisos de confidencialidad, los cuales pueden formalizarse mediante cláusulas en contratos, reglamentos internos, políticas institucionales o documentos específicos firmados, según corresponda al vínculo con la organización. Nivel 3: PD.6-5: Están definidas y documentadas qué conductas constituyen violaciones al principio de reserva. PD.6-6: Existe un procedimiento formalizado para investigar violaciones al principio de reserva. Nivel 4: PD.6-7: Toda solicitud interna de acceso a datos personales debe indicar la finalidad específica de uso y ser aprobada por los responsables designados.
Guía de implementación	La organización y terceros autorizados que accedan a datos personales dentro de su ámbito laboral, deberán utilizar esta información de forma reservada y únicamente para fines específicos vinculados a su actividad o giro habitual. Queda terminantemente prohibida la divulgación de datos a partes no autorizadas, asegurando así la protección de la privacidad de los titulares. Quienes, por su rol laboral o relación con el responsable de la base de datos, intervengan en cualquier fase del tratamiento de los datos, deben mantener un estricto secreto profesional, tal como lo estipula el artículo 302 del Código Penal. Es importante destacar que los funcionarios públicos tienen implícita la reserva en su relación funcional, así como los dependientes en su relación laboral.
Instituciones de salud	La historia clínica contiene información sensible y su acceso debe restringirse exclusivamente a personal involucrado en la atención médica (personal médico o administrativo), el usuario, en determinadas circunstancias familiares cercanos, y el Ministerio de Salud Pública.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Listado de usuarios, rol y permisos sobre datos a tratar. • Matrices de control de acceso a los datos personales para las bases involucradas. • Política de control de acceso lógico.
Normativa asociada	Ley 18.331: Protección de datos personales y habeas data. Código penal, articulo 302 sobre secreto profesional

Requisito PD.7	Principio de responsabilidad proactiva

Objetivo	Garantizar la seguridad en el tratamiento de datos por medio de medidas proactivas tomadas por el delegado de protección de datos personales de la organización. En el ejercicio de una responsabilidad proactiva se deben adoptar medidas técnicas y organizativas apropiadas con el fin de garantizar un tratamiento adecuado de los datos y demostrar su efectiva implementación.
Controles	Nivel 1: PD.7-1: La organización ha definido criterios para incorporar medidas de privacidad por diseño y por defecto en la construcción o mejora de procesos, servicios o sistemas. Nivel 2: PD.7-2: El delegado de protección de datos personales asesora en el diseño e implementación de medidas técnicas y organizativas destinadas a incorporar los principios de privacidad por diseño y por defecto en la organización. Nivel 3: PD.7-3: Ante cambios en procesos, sistemas o incidentes de seguridad, se revisa de forma reactiva la efectividad de las medidas implementadas para garantizar la incorporación de los principios de privacidad por diseño y por defecto en la organización. Nivel 4: PD.7-4: Se revisa periódicamente la efectividad de las medidas destinadas a incorporar los principios de privacidad por diseño y por defecto en la organización. PD.7-5: Las revisiones dan lugar a ajustes de las medidas técnicas implementadas.
Guía de implementación	La organización debe adoptar una postura proactiva en la implementación de medidas técnicas y organizativas apropiadas, como privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar la seguridad y el tratamiento adecuado de los datos personales. Además, debe documentar estas medidas y su efectiva implementación para demostrar el cumplimiento de las normativas de protección de datos, asegurando así la privacidad y los derechos de los titulares de los datos en todo momento.
Instituciones de salud	-
Instituciones Emisoras de Dinero Electrónico (IEDE)	-
Guía de evidencia para auditoría	• Evidencia de controles implementados para cumplir con los principios de privacidad desde el diseño y privacidad por defecto. • Evaluación de impacto a la protección de datos para los nuevos sistemas que manejan datos personales.

	• Designación y comunicación de delegados si corresponde.
Normativa asociada	• Ley 18.331: Protección de datos personales y habeas data • Normativa complementaria y concordante.

Requisito PD.8	Derechos de los titulares de los datos
Objetivo	Garantizar los derechos por parte de los titulares de los datos.
Controles	Nivel 1: PD.8-1: Se reciben y atienden las solicitudes relacionadas con los derechos sobre datos personales de los usuarios. PD.8-2: Se han gestionado respuestas a solicitudes de titulares dentro del plazo legal. Nivel 2: PD.8-3: Se encuentra asignado personal encargado de recibir, procesar y responder las solicitudes vinculadas a los derechos de los titulares. PD.8-4: Las solicitudes y su tratamiento son registrados. Nivel 3: PD.8-5: Existe un procedimiento formal de gestión de las solicitudes de derechos de los titulares que contempla todos los derechos mencionados en la normativa (Información, Acceso, Actualización y Rectificación, Inclusión, Supresión, Impugnación de Valoraciones Personales) PD.8-6: Se encuentra definido un procedimiento para verificar la identidad del solicitante del derecho. PD.8-7: Los procedimientos para ejercer los derechos son difundidos a los titulares de los datos, el personal y terceras partes interesadas. Nivel 4: PD.8-8: Se definen indicadores sobre el procedimiento de gestión de solicitudes de derechos. PD.8-9: Se revisa periódicamente el procedimiento de gestión de solicitudes de derechos, se registran los desvíos o puntos de mejora. PD.8-10: Se implementan las mejoras al procedimiento de gestión de solicitudes de derechos en base a las revisiones periódicas.
Guía de implementación	La organización debe permitir ejercer el derecho de acceso a los titulares de manera gratuita cada seis meses. La organización tendrá un plazo de respuesta de cinco días hábiles a contar de la solicitud, por los medios que se hayan indicado. En caso de falta de respuesta se habilita la acción de Habeas Data o la denuncia ante el órgano de control (URCDP). **Derecho de información:** Obliga a informar de manera clara y precisa al titular de los datos sobre el propósito del tratamiento, la obligatoriedad de responder, las consecuencias de proveer datos o no, cualquier transferencia internacional de datos, y los criterios de tratamientos automatizados.

	Derecho de Acceso: Permite a cualquier persona, previa acreditación de identidad, acceder a la información sobre sí misma que posea el responsable del tratamiento. En el caso de personas fallecidas, el ejercicio del derecho de acceso corresponderá a cualquiera de sus sucesores universales, que acrediten debidamente esta calidad. **Derecho de Actualización y Rectificación:** Otorga al titular el derecho de modificar sus datos personales que resulten inexactos o incompletos a la fecha de ejercicio del derecho. **Derecho de Inclusión:** Faculta al titular para ser incluido en una base de datos cuando demuestre un interés legítimo o fundado, especialmente si la inclusión representa un beneficio para él. **Derecho de Supresión:** Permite solicitar la eliminación de datos cuyo tratamiento resulte ilegítimo, o sean inadecuados o excesivos, salvo cuando deban conservarse por razones históricas, estadísticas, científicas, o en el marco de relaciones contractuales que justifiquen su tratamiento. Se procede la eliminación o supresión de datos personales en los siguientes casos: • Perjuicios a los derechos e intereses legítimos de terceros. • Notorio error. • Contravención a lo establecido por una obligación legal. **Derecho a la Impugnación de Valoraciones Personales:** Protege contra decisiones basadas únicamente en el tratamiento automatizado de datos destinadas a evaluar aspectos de la personalidad del individuo, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros, y que tienen efectos jurídicos significativos sobre él. Ofrece al titular de los datos la posibilidad de impugnar tales actos o decisiones, garantizando el derecho a ser informado sobre los criterios de valoración y el programa utilizado en el tratamiento que fundamenta la decisión.
Instituciones de salud	En caso de que una persona cambie de institución o de sistema de cobertura asistencial, la nueva institución o sistema deberá recabar de la o del de origen la historia clínica completa del usuario. El costo de dicha gestión será de cargo de la institución solicitante y la misma deberá contar previamente con autorización expresa del usuario.
Instituciones Emisoras de Dinero Electrónico (IEDE)	-

Guía de evidencia para auditoría	• Procesos y procedimientos que permiten a los titulares hacer ejercicio de sus derechos. • Documento de solicitud de accesos a la información realizadas y procesadas para que pueda validarse que se cumple con los plazos correspondientes.
Normativa asociada	• Ley 18.331: Protección de datos personales y habeas data • Normativa complementaria y concordante.