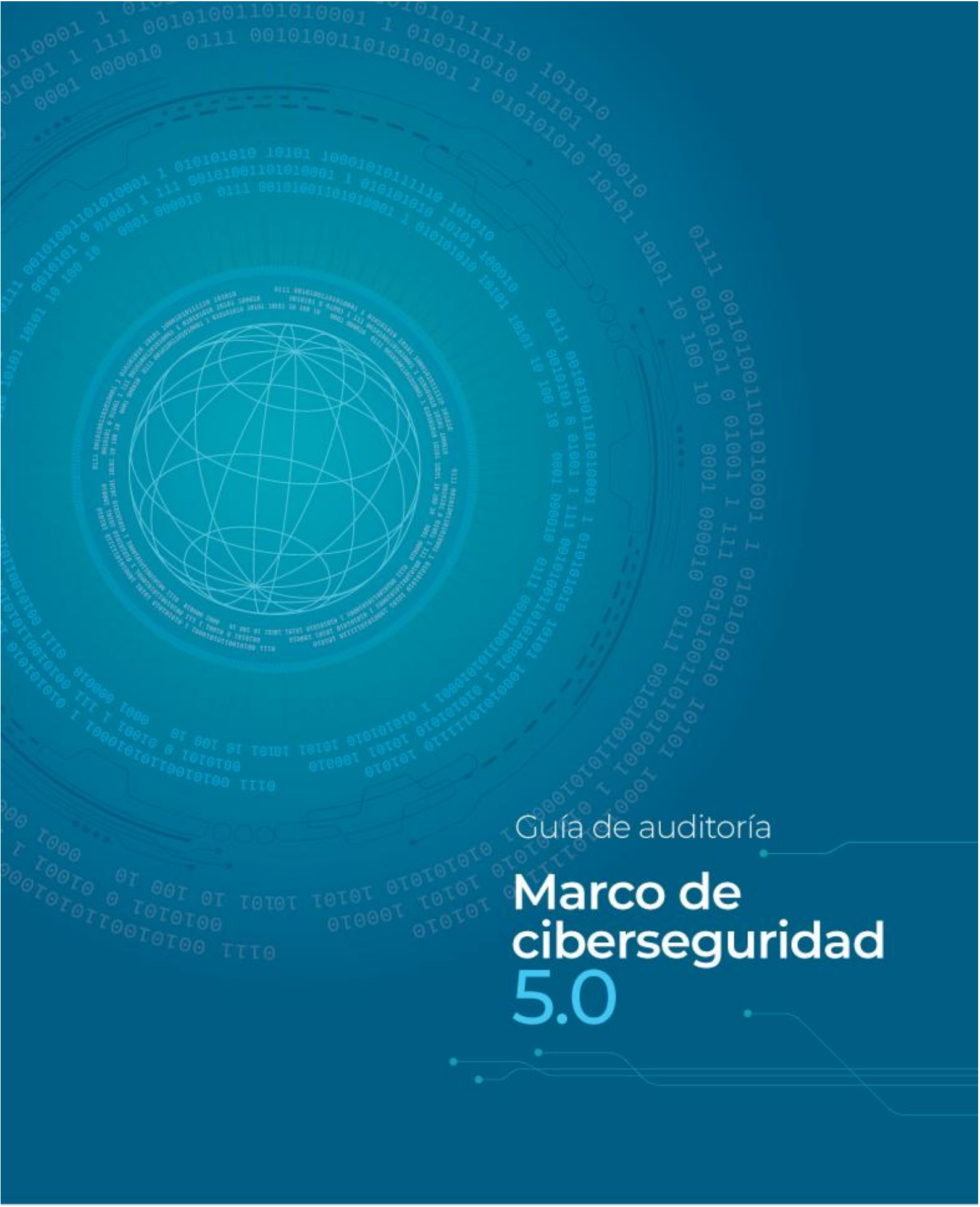

Guía de auditoría

Marco de ciberseguridad 5.0

Uruguay Presidencia | agesic

SEGURIDAD DE LA INFORMACIÓN

Versión 5.0 – Agosto 2025

1. Objetivo y alcance

Esta guía establece las pautas para el uso de las planillas de Perfil Comunitario, con la cual se evaluará el grado de adopción de los requisitos del Marco de Ciberseguridad y el nivel de madurez en el cual se encuentra la organización teniendo en cuenta el perfil asociado a la misma.

Todas las auditorías y/o evaluaciones que se realicen, utilizaran como marco de referencia el Marco de Ciberseguridad.

2. Mecanismo de auditoría

El Marco de Ciberseguridad puede ser auditado de diversas formas.
Autodiagnóstico: refiere a un diagnóstico o análisis de brecha realizado con el fin de conocer el estado de situación actual, el mismo podrá ser realizado por la misma organización o por terceras partes. No tiene como fin el cumplimiento normativo.
Autoevaluación: a los efectos de esta guía, se entiende como autoevaluación a un autodiagnóstico que tiene un fin de cumplimiento normativo, particularmente, al decreto 66/025. Esta autoevaluación será entregada a Agesic por las vías disponible a estos efectos.
Auditoria (interna o externa): proceso de relevamiento formal donde se evalúa por una tercera parte, el grado de implementación de los requisitos y su nivel de madurez. Esta evaluación puede ser realizada por el equipo de auditoria interna de la organización o por un equipo externo; además, podrá o no tener un fin de cumplimiento normativo.

3. Evaluación de requisitos

Los requisitos evaluados en la auditoria son los señalados en el Marco de Ciberseguridad. El cumplimiento de los requisitos se evalúa mediante la verificación de sus respectivos controles.

3.1 Cumplimiento de requisitos

La organización deberá demostrar la adopción o implementación de los requisitos a través de los siguientes medios:

1. Presentar la documentación e información adicional solicitada por el auditor durante el proceso de auditoría, dentro de los plazos establecidos en cada solicitud.
2. Permitir el libre acceso a los auditores a los recursos pertinentes a la auditoría.
3. Participar de las entrevistas que realice el auditor en el marco de las auditorias.
4. Presentar evidencia mediante vías de autoevaluación proporcionadas por Agesic, en cuyo caso deberá referenciarse al control evaluado.

La organización debe designar una contraparte para la auditoria, (sin importar si la misma es autoevaluación o auditoría. Esta persona debe participar activamente, por lo que deberá disponer del tiempo necesario para que la evaluación pueda ser hecha en los tiempos pautados.

3.2 Esquema de evaluación

La verificación de la implementación de los requisitos se realizará en conformidad a los siguientes elementos:

1. Comprender el contexto actual de la organización en relación con el uso de tecnologías de la información y seguridad de la información.
2. Visitas a las instalaciones.
3. Evaluación de la información obtenida.
4. Elaboración de informe.

4. Evaluación de madurez

Se realiza un relevamiento de todos los niveles de cada subcategoría propuesto en el modelo de madurez definido en el Marco de Ciberseguridad, indicando para cada subcategoría que nivel está cumpliendo.

Se debe recordar que los niveles superiores dan por cumplido los niveles inferiores. Por ejemplo, si en la subcategoría GV.OC-01 se indica el cumplimiento del nivel 3, implica que se cumple con el nivel 1 y 2.

Si no se verifica la adopción de todos los controles establecidos para el nivel 1, corresponderá asignar el nivel 0 a la subcategoría.

El cálculo de madurez se realiza mediante el promedio simple de los valores de madurez de las subcategorías incluidas en el alcance evaluado.
Por ejemplo:

- Para obtener el nivel de madurez de una categoría, se debe calcular el promedio simple de las subcategorías que la componen.
- Para obtener el nivel de madurez de una función, se debe calcular el promedio simple de todas las subcategorías asociadas a dicha función.
- Para el cálculo del nivel de madurez global, se debe calcular el promedio simple de todas las subcategorías del marco de ciberseguridad.

En ningún caso se deberá hacer promedio de promedios.

5. Evidencia

5.1 Organización y Gobernanza

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito PS.1 - Adoptar una Política de seguridad de la información

1. Resolución, registros u otro mecanismo que evidencie la aprobación de la Política de Seguridad de la Información por la dirección.
2. Registro de difusión de la Política de Seguridad de la Información (correo masivo, publicaciones, reuniones, actas, etc.).
3. Extracto de la Política de Seguridad de la Información que identifique los responsables de su cumplimiento y sus atribuciones.
4. Capturas de pantalla o enlaces activos en intranet, sistemas de gestión documental, wiki institucional o repositorio corporativo donde se encuentre accesible la Política de Seguridad de la Información.
5. Actas, minutas, correos u otros registros que documenten la revisión de la Política de Seguridad de la Información a partir de cambios normativos o del contexto organizacional.
6. Actas, presentaciones, correos o informes que demuestren que los resultados de la revisión de la Política de Seguridad de la Información fueron comunicados al Comité de Seguridad de la Información (CSI).
7. Registros de correos, actas, publicaciones internas u otros medios que evidencien la nueva difusión de la Política de Seguridad de la Información tras su modificación.
8. Registro documental, como la Política de Seguridad de la Información o manual de gestión, donde se indique expresamente la periodicidad con la que debe revisarse la Política de Seguridad de la Información.
9. Registro de revisión de la Política de Seguridad de la Información por parte de la Dirección (minutas, actas, correos, formularios, otros).
10. Política de Seguridad de la Información, actas del CSI, correos formales, informes técnicos u otros registros donde se definan indicadores para evaluar la efectividad de la política.

Requisito OR.1 - Designar un Responsable de la Seguridad de la Información.

11. Documentación o comunicaciones internas (actas, correos, minutas) que indiquen quién cumple de hecho funciones de Responsable de Seguridad de la Información (RSI), aunque no exista aún una designación formal.
12. Correos, actas, minutas o planillas donde conste que el RSI coordina o ejecuta tareas vinculadas a la seguridad de la información.
13. Resolución, memorando, contrato u otro documento que formalice la designación del RSI en la organización.
14. Descripción de cargo, manual de funciones o documento oficial donde se detallen las responsabilidades del RSI, incluyendo gestión de seguridad, incidentes, riesgos, entre otras.
15. Difusión de la designación del rol de RSI (correo, sitio web, intranet, etc.).
16. Actas, planillas, correos o informes que evidencien que el RSI lidera o coordina las evaluaciones de riesgos, o delego dicha función a referentes designados.
17. Notificación de designación a Agesic (correo, etc.).
18. Actas, convocatorias, correos u otro registro que demuestre la participación del RSI en el Comité de Seguridad de la Información.
19. Planes anuales de seguridad firmados o presentados por el RSI, que incluyan objetivos, acciones e indicadores asociados.
20. Actas de reuniones estratégicas, correos de convocatoria, presentaciones o informes donde se evidencie la participación del RSI en procesos de planificación institucional o estratégica.

Requisito OR.2 - Conformar un Comité de Seguridad de la Información.
1. Resolución, acta, memorando u otro documento que establezca formalmente la creación del Comité de Seguridad de la Información en la organización.

2. Actas, órdenes del día, minutas o registros de convocatoria que evidencien la realización periódica de reuniones del CSI con temas tratados y asistentes.
3. Documento aprobado por la dirección (resolución, manual, reglamento, acta, etc.) que incluya expresamente las responsabilidades y atribuciones del CSI.
4. Reglamento interno, manual de funcionamiento, acta de constitución u otro documento donde se detallen las reglas operativas del CSI, como frecuencia de reuniones, quórum, roles y forma de decisión.
5. Actas, presentaciones, correos u otros documentos que evidencien que el CSI interviene en la definición del nivel de riesgo aceptable.
6. Actas, presentaciones, correos u otros documentos que evidencien que el CSI aprueba el plan de tratamiento de riesgos.
7. Actas, minutas, informes, órdenes del día, entre otros mecanismos que evidencien que el CSI revisa planes y políticas de seguridad y aprueba sus actualizaciones.
8. Actas, resoluciones o presentaciones donde conste que el CSI aprueba o valida la planificación estratégica en materia de seguridad de la información.
9. Documento emitido por el CSI (como actas, informes, etc.) que incluya indicadores definidos para evaluar su desempeño.
10. Actas, reportes o presentaciones donde el CSI analice sus propios indicadores y defina acciones de mejora o ajustes en su forma de operar.

Requisito OR.3 - Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.
1. Resoluciones internas, documento de roles y responsabilidades del RSI o referente designado, actas de asignación de funciones, organigramas funcionales o comunicaciones institucionales que indiquen explícitamente quién es el punto de contacto oficial.

2. Listado oficial de contactos de autoridades y equipos externos relevantes (como CERTuy, URCDP, CSIRT sectoriales), incluyendo nombre, cargo, canal de contacto y condiciones de uso.
3. Comunicaciones institucionales, campañas internas de concientización, manuales de usuario, capacitaciones o encuestas al personal que evidencien que se ha difundido la identidad y función del punto de contacto oficial.
4. Procedimientos, anexos del plan de respuesta a incidentes o listas de contactos documentadas con información técnica y operativa para contacto con autoridades (incluyendo criterios de activación y medios de comunicación oficiales).
5. Versiones históricas de listados de contacto, registros de revisión (con fecha y responsable), actas de reunión o tickets de mantenimiento documental que evidencien que los contactos han sido verificados y actualizados en los últimos 12 meses.

Requisito OR.4 - Abordar la seguridad de la información en la gestión de los proyectos.

1. Planilla, sistema de gestión de proyectos o documento institucional donde figure el listado de proyectos de la organización (en curso, finalizados y planificados), actualizado al momento de la auditoría.
2. Actas, correos o formularios donde se evidencie que el RSI, o quien él designe, interviene en la planificación o inicio de proyectos.
3. Contratos, pliegos, documentación del llamado u otros documentos vinculados a proyectos que incluyan cláusulas específicas sobre seguridad de la información.
4. 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.

5. Registros de realización y seguimiento de la evaluación de riesgos de los proyectos que incluyan riesgos relativos a la seguridad de la información.
6. Informes de avance de los proyectos donde se incluye puntos que tratan sobre la evaluación de los riesgos de seguridad de la información.
7. Actas de cierre, informes finales o listas de verificación donde se valide el cumplimiento de los requisitos de seguridad definidos para el proyecto.
8. Documentos de cierre de proyecto, informes retrospectivos o presentaciones que incluyan lecciones aprendidas relacionadas con la gestión de seguridad de la información.

Requisito OR.5 - Pautar el uso de dispositivos móviles.

1. Planilla, sistema de gestión de activos, reporte u otro mecanismo que contenga el inventario actualizado de dispositivos móviles asignados por la organización.
2. Capturas de pantalla, archivos de configuración del sistema operativo u otros mecanismos que evidencien la aplicación de al menos un factor de autenticación en los dispositivos móviles de la organización.
3. Manual, instructivo, procedimientos u otros documentos internos que establezcan normas de uso, cuidado, y seguridad de los dispositivos móviles.
4. Registros de correos, actas, cartelería, plataforma de capacitación o firma de acuse de recibo que demuestren la difusión de las pautas de uso al personal.
5. Informes de revisión, reportes de MDM, o capturas que evidencien la implementación de los requisitos de seguridad (como antimalware, cifrado de disco, bloqueo automático, y versión mínima de sistema operativo) en los dispositivos móviles.

6. Capturas de pantalla, configuración exportada o informes de la herramienta MDM que evidencien la capacidad de ejecutar el borrado remoto de datos en dispositivos móviles.
7. Inventario o listado de dispositivos personales autorizados, con información sobre titular, fecha de aprobación y uso permitido, acompañado de la solicitud o autorización documentada (formulario, correo, sistema de tickets).
8. Informes de revisión, capturas de pantalla o reportes de MDM que evidencien la aplicación de los controles de seguridad definidos por la organización en los dispositivos personales registrados.
9. Resolución, registros u otro mecanismo que evidencie la aprobación de la Política de uso aceptable de dispositivos móviles por el CSI o la dirección.
10. Registros, minutas, actas, correos, formularios u otros documentos que evidencien que se realiza la revisión periódica y actualización de la Política de uso aceptable de dispositivos móviles.
11. Registros de actualización, actas u otros mecanismos que evidencien la revisión y mejora de procedimientos relacionados al uso seguro de dispositivos móviles.

Requisito OR.6 - Establecer controles para proteger la información a la que se accede de forma remota.

1. Política, instructivo o procedimiento técnico que detalle los requisitos mínimos de seguridad exigidos para los dispositivos que acceden de forma remota.
2. Logs del sistema, registros del servidor VPN o plataforma de acceso remoto que incluyan, al menos, fecha, hora, usuario, dirección IP y recurso accedido.
3. Exportación de reglas del firewall, configuración de acceso VPN, ACLs (listas de control de acceso) o archivos de política de red donde se limite explícitamente el acceso remoto a un conjunto definido de recursos autorizados.

4. Registro de configuración de la solución Múltiple Factor de Autenticación (MFA) utilizada, capturas de pantalla del proceso de autenticación, o reportes de acceso donde se evidencie el uso de múltiples factores en los accesos remotos.
5. Formularios, correos o sistema de tickets, entre otros, donde conste que el responsable del activo aprueba explícitamente el acceso remoto solicitado antes de su habilitación.
6. Documento formal que describa el proceso para solicitar, evaluar, autorizar y revocar accesos remotos.
7. Resolución, descripción de roles o manual de funciones donde se designe quién tiene a cargo la asignación y control de accesos remotos.
8. Resolución, registros u otro mecanismo que evidencie la aprobación de la Política de control de acceso remoto por el CSI o la dirección.
9. Registros de accesos otorgados a proveedores con vencimiento explícito (fecha o evento) y evidencia de su revocación posterior (logs, tickets, expiración automática).
10. Manual de funciones, instructivo operativo, resolución, acta o flujo de proceso donde se indique que la gestión de accesos remotos se canaliza de forma centralizada a través de un área o responsable definido.
11. Informes de revisión, matrices de acceso, bitácoras de auditoría, tickets de revisión o planillas firmadas que evidencien la verificación periódica de los usuarios con acceso remoto, incluyendo la vigencia, necesidad del acceso, etc.
12. Actas, planes de mejora, ajustes de procedimientos u otras evidencias de toma de decisiones basadas en los resultados de las revisiones de accesos remotos.
13. Informes de auditoría interna, lista de verificación de control o reportes que verifiquen el cumplimiento efectivo de los procedimientos establecidos para el acceso remoto.

Requisito OR.7 - Conocer el contexto de la organización

1. Listado de servicios críticos, matriz de criticidad, actas de validación de servicios esenciales, registros de continuidad de negocio o documentos del Sistema de Gestión de Seguridad de la Información (SGSI) que identifiquen servicios clave.
2. Inventario de partes interesadas, matriz de proveedores críticos, análisis de impacto de terceros, contratos clasificados por criticidad o informes de evaluación de dependencias externas.
3. Diagramas de procesos, mapas de procesos operativos y de soporte, documentación de procesos ISO u otras metodologías (BPM, SIPOC), con su respectivo responsable designado.
4. Documentos de análisis FODA, informes PESTEL, actas de revisión de contexto, informes estratégicos con mención a factores que impactan la seguridad de la información, o entregables del comité de riesgos o del RSI.
5. Matriz de dependencias, diagramas de relación entre procesos y servicios, análisis de impacto en cascada, modelos de continuidad de negocio (por ejemplo, BIA) que evidencien relaciones entre actores y funciones clave.
6. Actas de revisión de contexto, cronogramas de actualización anual, versiones comparativas de análisis FODA o PESTEL, informes de auditoría interna o planes de mejora que reflejen cambios y adecuaciones en el contexto organizacional.

Requisito PL.1 - Establecer objetivos anuales con relación a la Seguridad de la Información.

1. Planes operativos, presentaciones institucionales, actas del CSI o de dirección donde se detallen objetivos anuales de seguridad de la información.
2. Planillas, planificaciones o mecanismos que detallen las acciones previstas para alcanzar los objetivos.

3. Objetivos de seguridad integrados en planes de acción institucionales, planes operativos anuales, cronogramas de ejecución, plataformas de seguimiento o presentaciones internas que vinculen objetivos con acciones, responsables y plazos.
4. Actas del CSI, minutas, correos de validación, registros en sistemas de gestión o presentaciones utilizadas en sesiones donde se haya discutido y aprobado formalmente el conjunto de objetivos anuales y su plan de ejecución
5. Correos masivos, publicaciones en intranet, presentaciones internas o constancias de reuniones donde se haya comunicado formalmente el contenido de los objetivos y sus metas asociadas.
6. Cronogramas de trabajo compartido, registros de reuniones, tickets o plataformas colaborativas donde se evidencie la participación de distintos sectores en la ejecución de acciones vinculadas a los objetivos.
7. Tableros de control, plantillas de indicadores, informes de seguimiento o secciones dentro del plan de acción que contengan métricas concretas asociadas a cada objetivo.
8. Cartera de proyectos, fichas técnicas, formularios de presentación, actas de aprobación u otros mecanismos donde se evidencie que los objetivos de seguridad se han transformado en proyectos específicos.
9. Informes de seguimiento, versionado del plan de acción, reportes de progreso o actas de revisión donde se analice el estado de cumplimiento de los objetivos y se ajusten las acciones según los resultados obtenidos.

5.2 Gestión de riesgos

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito GR 1 - Adoptar una metodología de evaluación de riesgo.

1. Procedimiento operativo, matriz de riesgos separada por servicio o componente, actas de evaluación, informes técnicos, reportes de consultoría o cualquier otro registro que evidencie la aplicación diferenciada del proceso de gestión de riesgos a servicios críticos o componentes del centro de procesamiento de datos.
2. Manual metodológico, instructivo operativo, plantilla con criterios aplicados, presentaciones de capacitación interna o informes de aplicación práctica que describan la metodología de gestión de riesgos de seguridad de la información (identificación, evaluación, tratamiento, seguimiento y comunicación a los interesados) utilizada por la organización.
3. Resolución, registros u otro mecanismo que evidencie la aprobación de la Política de gestión de riesgos de seguridad de la información por el CSI o la dirección.
4. Registro de correos institucionales, actas, firma de acuse de recibo, publicaciones internas, sitio institucional u otros mecanismos que evidencien que la política fue comunicada a todas las partes interesadas.
5. Versionado de la metodología, actas de revisión, informes de ajuste, análisis comparativo de versiones, o minutas que demuestren que la metodología fue revisada y ajustada en función de resultados previos, cambios normativos o de contexto, y oportunidades de mejora identificadas.

Requisito GR 2 - Realizar de manera sistemática el proceso de evaluación de riesgos.
1. Matrices de riesgo, planillas, informes de evaluación o reportes generados por herramientas donde conste la identificación de riesgos, su impacto estimado y probabilidad de ocurrencia.

2. Planillas, FODA, informes de análisis de riesgos o salidas de herramientas de gestión que detallen las amenazas y vulnerabilidades identificadas, así como los controles actuales implementados para su mitigación.
3. Matriz de riesgos, sistema de gestión o planilla donde se detallen los riesgos asociados a cada activo de información de la organización.
4. Resoluciones, actas del Comité de Seguridad o informes validados por la dirección donde se establezcan el apetito de riesgo y la tolerancia al riesgo de la organización.
5. Informes de evaluación de riesgos o matrices donde se incluyan explícitamente riesgos relacionados con proveedores, contratos, servicios tercerizados o interdependencias externas.
6. Registros que evidencien que incidentes ocurridos fueron utilizados como insumo para la actualización de riesgos, como su incorporación en matrices, informes de reevaluación o ajustes en planes de tratamiento.
7. Actas, registros de revisión o informes donde conste que la tolerancia al riesgo fue revisada y ajustada ante cambios normativos, tecnológicos o estratégicos.
8. Versiones anteriores y actualizadas de la matriz de riesgos o listado equivalente, con registro de fecha, responsable y cambios realizados, acompañadas de actas, tickets o informes que respalden la revisión periódica realizada.

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.

1. Correos, tickets, actas o informes que evidencien la toma de acciones puntuales para reducir riesgos identificados.
2. Planes de tratamiento de riesgos, matrices o registros que incluyan acciones definidas para riesgos que superan los límites aceptables.

3. Registros de planes de tratamiento de riesgos que detallen cada acción, su responsable designado y el plazo previsto para su ejecución.
4. Actas, correos de aprobación, tickets o plataformas colaborativas donde se evidencie que quienes ejecutan las acciones validaron el contenido del plan de tratamiento de riesgos antes de su implementación.
5. Planillas, tableros o dashboards o informes donde se incluyan métricas e indicadores definidos para hacer seguimiento del avance de los planes de tratamiento.
6. Resoluciones, actas o comunicaciones donde la Dirección establezca el orden de ejecución de acciones o controles.
7. Informes de verificación, pruebas de control, auditorías internas o matrices actualizadas con análisis del riesgo residual, junto con registros de validación por las partes interesadas.
8. Presupuesto institucional, partidas asignadas, plan financiero, resoluciones de asignación de fondos o planillas presupuestales que evidencien que existe una línea presupuestal específica (o rubro identificado) destinada a implementar medidas del plan de tratamiento de riesgos de seguridad de la información.
9. Versionado de planes, informes de seguimiento, actas o herramientas que reflejen la revisión de los planes en forma periódica, incluyendo fecha y responsables de la actualización.
10. Actas del CSI, correos formales, informes ejecutivos o presentaciones que evidencien que los cambios o resultados de revisión fueron compartidos con las partes interesadas relevantes.

Requisito GR.4 - Inteligencia de amenazas

1. Registro de las fuentes utilizadas para recibir inteligencia de amenazas, como CERTuy, portales oficiales, fuentes sectoriales o comunitarias.
2. Registros de asistencia a capacitaciones, materiales de formación o certificados vinculados a cursos específicos sobre análisis o uso de inteligencia de amenazas recibidos por el personal.

3. Registros que demuestren la recepción periódica de información sobre amenazas (como alertas por correo, boletines, feeds RSS o reportes de herramientas SIEM, entre otros), junto con planillas, tickets o sistemas internos donde se almacene dicha información para su análisis posterior.
4. Manuales de responsabilidades y funciones, resolución, organigramas, o flujos de proceso donde se identifiquen claramente los responsables de recibir, filtrar y analizar la información de amenazas.
5. Informes, matrices, presentaciones o actas donde se haya evaluado el posible efecto de amenazas recientes o nuevas tendencias sobre activos o servicios que también utiliza la organización.
6. Registros de reuniones, actas del comité de seguridad, actualizaciones del análisis de riesgos, informes de evaluación o matrices de riesgo donde se evidencie que los datos provenientes de inteligencia de amenazas han sido utilizados como insumo para ajustar la probabilidad, impacto o tratamiento de riesgos de seguridad de la información.
7. Procedimiento formal vigente, manual operativo, instructivo o política específica que describa cómo se gestionan las fuentes de inteligencia de amenazas, incluyendo los mecanismos para su recepción, criterios para el filtrado y validación, métodos de análisis y clasificación de la información, y su utilización.
8. Planes de tratamiento de riesgos, informes de análisis, actas de comité de seguridad, registros de revisión de controles o reportes de adecuación que demuestren que la información proveniente de inteligencia de amenazas ha sido utilizada para ajustar controles existentes o diseñar nuevos controles.
9. Actas, registros de revisión o informes donde se evalúe la vigencia, confiabilidad y relevancia de las fuentes utilizadas.
10. Matrices de riesgo, planes de tratamiento o informes de reevaluación donde consten actualizaciones realizadas en función de nueva información proveniente de inteligencia de amenazas, incluyendo fecha del cambio y fuente que lo motivó.

11. Presentaciones, informes ejecutivos o registros de reuniones donde se utilicen patrones o tendencias observadas en la inteligencia de amenazas como base para decisiones estratégicas.

5.3 Gestión humana

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

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.

1. Contratos laborales, estatutos, convenios colectivos o normativa interna donde figuren cláusulas específicas vinculadas a obligaciones del personal respecto a la seguridad de la información.
2. Manuales de funciones, descripciones de cargo, anexos contractuales, guías de inducción o políticas específicas que asignen responsabilidades de seguridad al personal según su rol.
3. Formularios de acuse de recibo, registros de inducción, plataformas de inducción o lista de verificación de ingreso donde conste que el nuevo personal fue informado sobre sus responsabilidades en seguridad de la información.
4. Procedimiento formal que contemple los pasos a seguir ante la desvinculación, incluyendo baja de accesos, recuperación de activos y lista de verificación de salida.
5. Reglamento interno, instructivo de sanciones o resolución que defina las consecuencias ante incumplimientos de políticas de seguridad
6. Versionado de contratos, registros de revisión de estatutos o cláusulas tipo, con fecha, responsables y resultados de los ajustes realizados.
7. Versiones comparadas de contratos, cláusulas de seguridad, manuales de ingreso o procedimientos de desvinculación, junto con registros de revisión que incluyan fecha, responsables y observaciones, como

tickets de actualización o informes del área de gestión humana, legal o seguridad de la información.

8. Planillas, informes, tickets o reportes donde se lleve un seguimiento de incumplimientos contractuales vinculados a la seguridad de la información.

Requisito GH.2 - Concientizar y formar en materia de seguridad de la información a todo el personal.

1. Correos institucionales, publicaciones en intranet, cartelería, boletines o presentaciones utilizadas para comunicar políticas de seguridad, buenas prácticas o mecanismos de protección al personal.
2. Presentaciones, infografías, videos, manuales, trivias, simulacros de phishing u otros recursos utilizados o adquiridos para campañas de concientización.
3. Cronogramas, briefings, guías de implementación o kits de comunicación donde conste la planificación y diseño de campañas internas de sensibilización.
4. Calendario de actividades aprobado, plan anual o plan semestral que defina fechas, temas, responsables y canales para ejecutar las campañas de concientización.
5. 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.
6. Actas del CSI o de dirección, presentaciones institucionales, correos de validación o registros de seguimiento donde conste la aprobación formal de las campañas, con sus indicadores definidos.
7. Planes de formación en seguridad, cronogramas difundidos por correo institucional, publicaciones en la intranet o wiki interna, registros cargados en plataformas o presentaciones internas utilizadas para

comunicar la planificación de concientización y capacitación relacionada a seguridad de la información.

8. Resultados de tests, encuestas, actividades de retroalimentación o simulaciones aplicadas al personal luego de cada campaña o instancia formativa.
9. Actas, correos formales o presentaciones donde se registre que el plan o campañas fueron validadas por el CSI y respaldadas explícitamente por instancias directivas.
10. Versiones sucesivas del plan de capacitación, informes de actualización, tickets de ajuste, presentaciones internas o actas donde se registre la revisión y modificación del plan de concientización y capacitación en seguridad de la información.

Requisito GH.3 - Concientizar y formar en materia de seguridad de la información al personal que desempeña funciones especializadas.

1. Resultados de entrevistas, evaluaciones, formularios de validación, encuestas internas o actividades de retroalimentación donde se evidencie que los usuarios privilegiados comprenden la importancia de sus responsabilidades.
2. Encuestas respondidas, evaluaciones de conocimiento, entrevistas o simulacros donde se refleje el nivel de concientización del personal de seguridad sobre su rol en la seguridad de la organización.
3. Contratos, acuerdos de nivel de servicio, cláusulas de seguridad, instructivos operativos o anexos donde se establezcan las responsabilidades en materia de seguridad de terceros o proveedores.
4. Cronogramas de concientización para usuarios privilegiados, materiales utilizados en las campañas diferenciadas, registros de asistencia o presentaciones enfocadas en riesgos y buenas prácticas para usuarios privilegiados.
5. Registros de sesiones de capacitación, calendarios de actividades internas, presentaciones específicas o reportes de campañas dirigidas

al personal de seguridad física y al equipo de seguridad de la información.

6. Boletines informativos, material explicativo, actividades de inducción o presentaciones entregadas a terceros para comunicar roles y obligaciones en seguridad.
7. Registros de asistencia, capturas de pantalla, presentaciones lideradas por gerencia o menciones formales en comunicados donde se refleje la participación activa de la gerencia en iniciativas de concientización.
8. Registros de inscripción o finalización de cursos, certificados, agenda de talleres o correos de invitación a capacitaciones específicas orientadas a perfiles con privilegios elevados.
9. Certificados de formación, registros de participación, agendas de eventos, o materiales entregados en cursos avanzados destinados a personal de seguridad física o de la información.
10. Registros de sesiones de inducción, instructivos firmados, encuestas de comprensión, validación de conocimiento o lista de verificación de capacitación para terceros que acceden o manejan información sensible de la organización.
11. Planes de formación segmentados por perfil, cronogramas diferenciados, fichas de planificación o reportes que evidencien el diseño de actividades considerando intereses y riesgos específicos de grupos clave como tecnología, gestión humana o usuarios con acceso privilegiado, entre otros.

5.4 Gestión de activos

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito GA.1 - Identificar formalmente los activos de la organización junto con la definición de su responsable.
1. Planillas de control, exportaciones de herramientas, capturas de sistemas de gestión o registros internos entre otros mecanismos que

evidencien que los servidores, racks, UPS, dispositivos de red y otros componentes físicos del centro de procesamiento de datos se encuentran inventariados.

2. Reportes generados por herramientas de gestión de activos o descubrimiento automático de software, planillas internas, scripts de auditoría o capturas del sistema de gestión de activos, entre otros mecanismos que evidencien que el software base y de aplicación instalado en los activos del centro de procesamiento de datos se encuentra debidamente inventariado.
3. Planillas de inventario, registros del sistema de gestión de activos, formularios de asignación o capturas de plataformas utilizadas, donde cada activo cuenta con un responsable asignado y documentado.
4. Planillas de control, reportes de sistemas de gestión de activos, capturas de herramientas de descubrimiento automático o formularios de alta de equipos, entre otros registros que evidencien que todos los dispositivos físicos utilizados dentro y fuera del centro de procesamiento de datos están inventariados.
5. Listados técnicos, planillas internas, reportes de herramientas de gestión o plataformas de administración de licencias, que reflejen que se mantiene un inventario actualizado de software y aplicaciones.
6. Planillas de seguimiento, reportes automatizados, formularios de adquisición o registros de auditoría que permiten verificar que se gestiona activamente el licenciamiento del software, incluyendo información sobre tipo, vigencia y uso asignado.
7. Capturas de plataformas de gestión con control de accesos configurado, registros de permisos, actas de definición de perfiles o documentación interna de seguridad que acrediten que el inventario está disponible exclusivamente para las personas autorizadas por la organización.
8. Políticas de gestión de activos, diagramas de flujo, procedimientos operativos normalizados o instructivos de trabajo que detallen cómo se mantiene actualizado el inventario de activos, demostrando que existen lineamientos formales definidos por la organización.

9. Capturas de pantalla, reportes de uso, manuales internos o fichas técnicas del sistema implementado que permitan constatar que la organización utiliza una herramienta específica para registrar, rastrear y controlar sus activos tecnológicos y de información.
10. Configuraciones de herramientas con agentes instalados, flujos automatizados documentados, registros generados por scripts programados o capturas de tareas programadas, utilizados para verificar que el proceso de actualización del inventario incluye mecanismos automáticos, ya sea total o parcialmente.
11. Reportes periódicos de control, alertas automáticas, paneles de monitoreo de licencias o registros de revisión de cumplimiento, que permitan confirmar que se realiza un seguimiento continuo del estado del licenciamiento y se detectan a tiempo los vencimientos o irregularidades.
12. Informes de auditoría interna, cronogramas de revisión, listas de verificación utilizadas, reportes de hallazgos o planes de acción generados, que evidencien que se realizan auditorías periódicas sobre el inventario para evaluar el cumplimiento de las políticas y procedimientos definidos.
13. Planillas de inventario de software, reportes de escaneo de versiones, registros de gestión de vulnerabilidades, tickets de remoción o actas de comité técnico que evidencien que el software fuera de soporte, o que representa un riesgo no aceptable según el análisis de seguridad, ha sido eliminado de los sistemas o reemplazado por versiones soportadas o alternativas seguras.
14. Inventario actualizado con fechas de fin de soporte, registros de baja de activos, informes de análisis de obsolescencia, actas del CSI o reportes del RSI que documenten la decisión de eliminación, cronogramas de reemplazo, y reportes de escaneo que identifiquen versiones sin soporte eliminadas del entorno.

Requisito GA.2 - Clasificar y proteger la información de acuerdo con la normativa y a los criterios de valoración definidos.
1. Listas de activos priorizados, matrices de criticidad, planillas internas o reportes generados por el área de seguridad, entre otros mecanismos que demuestren que se han identificado los activos que contienen información crítica conforme a criterios definidos por la organización. 2. Campos configurados en el sistema de gestión de activos, planillas con columnas de clasificación, capturas de pantalla o formularios de registro que indiquen que cada activo tiene asignada su clasificación según los criterios establecidos. 3. Inventarios donde se visualice la clasificación aplicada, reportes de revisión de activos clasificados, formularios de registro o tickets de alta que reflejen que los activos que almacenan o procesan información han sido clasificados de acuerdo con el procedimiento institucional. 4. Capturas de pantalla, manuales de usuario, fichas de configuración o reportes generados por la herramienta de gestión de activos, que evidencien que el sistema permite registrar, consultar y mantener la clasificación de cada activo. 5. Política formal, instructivo interno o procedimiento operativo firmado o validado por la organización, que establezca los criterios y niveles de clasificación alineados con la normativa nacional vigente. 6. Instructivos o diagramas de flujo que definan cómo se etiquetan los activos. 7. Formularios de alta, tickets de modificación, procedimientos de baja y configuraciones del sistema que reflejen la incorporación del criterio de clasificación en todas las etapas de gestión de los activos. 8. Configuraciones de sistemas, matrices de control de accesos, registros de asignación de permisos o instructivos técnicos que permitan demostrar que los accesos a la información están definidos en función de la clasificación de los activos y los perfiles autorizados. 9. Informes de revisión interna, lista de verificación, registros de auditoría o reportes de monitoreo que acrediten que se realizan controles

periódicos para validar que la clasificación aplicada a los activos sigue siendo correcta y actualizada.

Requisito GA.3 - Pautar el uso aceptable de los activos.

1. Instructivos, manuales de usuario, guías operativas, mensajes institucionales o registros de comunicación interna que permitan comprobar que existen pautas básicas de uso aceptable de los activos de información definidas por la organización.
2. Formularios de aceptación firmados, registros de consentimiento en plataformas de inducción, contratos con cláusulas específicas o sistemas con validación previa al primer acceso, que evidencien que toda persona debe aceptar formalmente las condiciones de uso antes de acceder a activos de información.
3. Instructivos técnicos, políticas de uso, configuraciones de herramientas de cifrado o control de acceso y listas de activos restringidos, que demuestren que se prohíbe o regula el almacenamiento de información sensible en activos sin controles adecuados.
4. Políticas de uso, configuraciones de herramientas de gestión de dispositivos, controles técnicos en endpoints o registros de incidentes bloqueados, que evidencien que existen medidas técnicas o administrativas para impedir acciones como la instalación de software no autorizado o el cambio de configuraciones críticas.
5. Documento de Política de uso aceptable de los activos aprobado por la dirección, incorporado en normativas internas, planificaciones institucionales o publicaciones oficiales, que evidencie la existencia de una política formal que regule el uso adecuado de los activos de información.
6. Correos institucionales, registros de comunicación en la intranet, materiales de sensibilización o listas de distribución, que demuestren que la política de uso ha sido comunicada al personal, proveedores y terceros.

7. Informes de revisión, cronogramas de controles, listas de verificación o tickets de seguimiento que demuestren que se realiza una supervisión periódica de los activos que contienen o procesan información sensible.
8. Planes de contingencia, procedimientos específicos de respuesta, formularios de notificación o simulacros realizados, que demuestren que existe un plan formal para actuar ante la pérdida o robo de activos de información.
9. Registros de actividad de herramientas de monitoreo, reportes de SOC, configuraciones de alertas o contratos con proveedores de servicios gestionados, que evidencien que las medidas de protección implementadas en los activos son monitoreadas permanentemente.
10. Informes de revisión, auditorías internas, controles aleatorios, listas de chequeo o reportes de hallazgos que evidencien que se realizan evaluaciones periódicas para verificar que el uso de los activos se ajusta a lo definido en la política.

Requisito GA.4 - Gestionar los medios de almacenamiento externos.

1. Correos institucionales, publicaciones en intranet, cartelería interna, materiales de concientización o presentaciones utilizadas para sensibilizar sobre la importancia de proteger y utilizar de forma segura los medios de almacenamiento externos.
2. Listados de medios autorizados, actas de definición, instructivos técnicos, manuales de uso o entradas en sistemas de gestión, que evidencien que la organización ha definido e identificado los tipos de medios de almacenamiento externos habilitados para su uso.
3. Instructivos, manuales operativos, presentaciones de sensibilización, publicaciones en canales internos o correos masivos que demuestren que se han establecido y comunicado las pautas de uso seguro para medios de almacenamiento externos.
4. Planillas, registros en herramientas de gestión, etiquetas físicas o digitales, o formularios internos que permitan verificar que los medios

de almacenamiento externo están inventariados y clasificados según la información que contienen y sus características técnicas.

5. Procedimientos operativos, protocolos de respuesta, materiales de comunicación, formularios o instructivos difundidos que detallen las acciones específicas ante la pérdida, hurto o daño de un medio externo y su distribución a los interesados.
6. Documento de política aprobado y vigente, procedimiento operativo formalizado, publicaciones oficiales o versiones registradas en sistemas de gestión, que evidencien que la organización cuenta con una política y procedimiento para la gestión de medios de almacenamiento externos.
7. Informes de control interno, listado de verificación de auditoría, reportes de cumplimiento o actas de revisión que permitan verificar que se evalúa regularmente el cumplimiento de las pautas, la política y el procedimiento aplicables a los medios de almacenamiento externos.
8. Registros de ajustes realizados, versiones comparadas, comunicaciones al RSI, actas de comités o correos formales que evidencien que los resultados de las revisiones se utilizan para mejorar la política y el procedimiento, y que estas mejoras son comunicadas a los responsables y partes interesadas.

Requisito GA.5 - Establecer los mecanismos para destruir la información y medios de almacenamiento.

1. Instructivos operativos, guías internas, procedimientos simplificados o publicaciones institucionales que indiquen cómo debe realizarse el borrado seguro o la disposición final de los medios de almacenamiento.
2. Campañas de concientización, correos institucionales, afiches internos, publicaciones en la intranet o presentaciones utilizadas para comunicar la necesidad de eliminar correctamente los medios de almacenamiento que ya no se utilizarán.
3. Planillas internas, esquemas operativos, asignaciones de roles o cartelería en puntos específicos que indiquen las personas o

ubicaciones autorizadas para llevar a cabo la eliminación segura de medios.

4. Instructivos técnicos, flujos de decisión, cuadros de referencia o guías de uso interno que especifiquen los criterios bajo los cuales se decide aplicar destrucción lógica, física o combinada sobre los medios de almacenamiento.
5. Documento de política vigente, aprobado por la dirección, publicado en los canales oficiales o incorporado en el marco normativo interno, que defina los principios y lineamientos sobre la destrucción de la información.
6. Procedimiento operativo validado, con detalle de roles, métodos permitidos, etapas del proceso y registros requeridos, que permita verificar que existe un método formalmente establecido para la destrucción de la información.
7. Planillas, formularios de destrucción, registros firmados, sistemas internos o tickets que documenten fecha, tipo de medio, técnica utilizada y personal involucrado en cada actividad de destrucción.
8. Resultados de pruebas de borrado, certificados de destrucción, informes de validación o controles cruzados que evidencien que la organización evalúa la efectividad de los métodos aplicados en la destrucción de información.
9. Informes de control interno, listas de verificación, hallazgos de auditoría o reportes de revisión que permitan constatar que se evalúa periódicamente el cumplimiento del procedimiento establecido para la destrucción de medios e información.

5.5 Control de acceso

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito CA.1 - Gestión de identidades y credenciales

1. Configuraciones del sistema, capturas de pantallas, reportes de seguridad o documentación técnica que evidencien que todos los sistemas requieren autenticación para acceder.
2. Listados de cuentas, registros de acceso, configuraciones de usuarios o políticas internas que demuestren que el acceso a redes y sistemas se realiza únicamente con usuarios identificables y asignados a personas específicas.
3. Listados actualizados de usuarios con privilegios, registros de monitoreo, configuraciones de roles o reportes de acceso que evidencien que el uso de cuentas privilegiadas está sujeto a control.
4. Configuraciones de autenticación, reportes técnicos, capturas de sistemas o instructivos que permitan verificar que el acceso a aplicaciones se realiza mediante mecanismos de autenticación seguros.
5. Formularios de excepción, resoluciones internas, actas de autorización o tickets de solicitud que permitan verificar que el uso de usuarios genéricos está justificado, controlado y autorizado formalmente por la organización.
6. Instructivos operativos, formularios con campos de aprobación, flujos de proceso o tickets que reflejen que existen reglas claras para el alta, baja o modificación de accesos lógicos, incluyendo las aprobaciones correspondientes.
7. Listados de sistemas críticos, análisis de riesgos, matrices de categorización o criterios de seguridad donde se identifiquen los

escenarios que requieren autenticación fuerte y los controles definidos para ellos.

8. Configuraciones de cifrado, políticas técnicas, auditorías internas, pruebas de seguridad o documentación de arquitectura que evidencien que las credenciales están protegidas en tránsito y en reposo mediante mecanismos criptográficos robustos.
9. Política aprobada, manual de seguridad, publicación interna o presentación institucional que establezca los criterios para la gestión de usuarios y contraseñas, y su comunicación formal al personal.
10. Procedimientos formalizados, instructivos, diagramas de flujo o registros operativos que detallen cómo se realiza el alta, baja y modificación de usuarios dentro de la organización.
11. Configuraciones de sistemas de identidad, capturas de plataformas, informes técnicos o actas que acrediten que la gestión de credenciales se realiza desde una única área o sistema, al menos de forma administrativa.
12. Configuraciones del sistema, documentación de arquitectura, pruebas de integridad o capturas de logs que demuestren que los tokens utilizados (como SAML assertions o JWTs) son validados en cada uso y se verifica su integridad.
13. Informes de auditoría, registros de monitoreo, alertas automatizadas, listas de verificación o cronogramas de control que permitan comprobar que se realizan revisiones periódicas sobre autenticación y configuración de accesos en redes, sistemas y dispositivos.

14. Versiones anteriores de la política y/o procedimientos, registros de revisión (actas, correos, tickets, informes de actualización), cronogramas de revisión aprobados, comentarios de revisión del RSI o del CSI, y controles de cambio documentados que evidencien la periodicidad de la revisión y los ajustes realizados.

Requisito CA.2 - Revisar los privilegios de acceso lógico.

1. Tickets de baja o modificación, registros de gestión de accesos, planillas internas o flujos de proceso aplicados en casos concretos que permitan verificar que, ante una baja o cambio, se revisan los privilegios al menos en los sistemas críticos.
2. Políticas internas, cronogramas de control, instructivos operativos o comunicaciones institucionales que establezcan cada cuánto se debe revisar la validez de las cuentas y privilegios asignados.
3. Manuales de funciones, resoluciones, matrices de asignación de roles o flujos de procedimiento donde se indique quién es responsable de revisar privilegios y validar cuentas por cada sistema o área.
4. Listados generados desde sistemas, reportes de plataformas de identidad, planillas de control o registros firmados por responsables que permitan comprobar que se mantiene un inventario actualizado de usuarios con privilegios elevados, incluyendo validación de su vigencia.
5. Política formal vigente que incluya cláusulas sobre la revisión periódica de privilegios de todos los usuarios, en todos los sistemas, aprobada por las instancias correspondientes y difundida institucionalmente.

6. Procedimientos operativos o instructivos que detallen cómo se realizan las revisiones de permisos en cada etapa del ciclo de vida de los usuarios (alta, modificación, baja), incluyendo usuarios privilegiados.
7. Planillas de control, logs de revisión, reportes de cumplimiento, tickets u otros registros que evidencien que las revisiones de accesos efectivamente se ejecutan y quedan registradas.
8. Informes de revisión con resultados, registros de envío, actas de reuniones, correos o presentaciones que demuestren que los resultados son documentados y comunicados al RSI, gerencias y demás partes interesadas.
9. Actas, correos institucionales, informes de seguimiento o presentaciones utilizadas para formalizar la entrega de los resultados de las revisiones de privilegios a las áreas correspondientes.
10. Informes de auditoría interna, planes de auditoría, hallazgos identificados o listas de verificación que permitan verificar que se audita periódicamente el cumplimiento del procedimiento de revisión de privilegios y de lo establecido en la política de control de acceso lógico.

Requisito CA.3 - Establecer controles criptográficos.

1. Listados de respaldos críticos, instructivos internos o documentación de arquitectura que identifiquen qué datos históricos y respaldos deben protegerse mediante controles criptográficos u otros mecanismos seguros.

2. Configuraciones del sistema de respaldo, reportes de herramientas de respaldo, capturas de configuración, registros de procesos o documentación técnica que permitan verificar que los respaldos offline o datos históricos se almacenan en forma cifrada.
3. Manuales técnicos, configuraciones de herramientas, instructivos de seguridad o fichas técnicas de implementación que detallen los algoritmos, longitudes de clave y protocolos utilizados en los mecanismos criptográficos de la organización.
4. Documento de política vigente, aprobado y difundido internamente, que defina los lineamientos para el uso de criptografía en la organización.
5. Matrices de roles, manuales de funciones, actas de designación o procedimientos donde se especifique quiénes son los responsables de generar, custodiar, renovar y revocar las claves criptográficas, cubriendo todo su ciclo de vida.
6. Informes de control interno, listas de verificación, planes de revisión o registros de auditoría que evidencien que se evalúan periódicamente los controles criptográficos implementados para asegurar su adecuación y eficacia.
7. Informes de revisión firmados, correos institucionales, minutas de reunión o presentaciones que permitan comprobar que los resultados de las revisiones criptográficas fueron registrados e informados al Responsable de Seguridad de la Información.
8. Diagrama de arquitectura, configuraciones de HSM, plataformas de gestión de llaves, políticas criptográficas o registros de custodia, que

permitan verificar que la organización gestiona las claves criptográficas de forma centralizada.

Requisito CA.4 - Establecer los controles para el uso de firma electrónica.

1. Listados de sistemas, matrices de requerimientos, relevamientos funcionales, flujos de proceso o informes de análisis que evidencien que la organización ha identificado qué procesos y sistemas requieren el uso de firma electrónica avanzada.
2. Capturas de configuración, documentación técnica, manuales del sistema o reportes de validación que permitan comprobar que los sistemas implementan certificados X.509v3 emitidos por prestadores acreditados por la UCE.
3. Informes de configuración de sistemas, análisis de seguridad, pruebas de penetración o documentación técnica que demuestren que se utilizan protocolos criptográficos seguros.
4. Configuraciones del sistema, documentación técnica, informes de cumplimiento o ejemplos de documentos firmados que reflejen el uso de estándares adecuados como XAdES, PAdES o PDFSignature, según corresponda.
5. Logs de verificación, configuraciones del sistema, reportes técnicos o capturas de herramientas que evidencien que los certificados electrónicos son validados mediante OCSP, CRL o mecanismos equivalentes.
6. Funcionalidades implementadas, reportes de error, bitácoras del sistema o manuales que permitan constatar que la solución detecta firmas inválidas, rotas o alteradas, y mantiene trazabilidad de los eventos asociados.
7. Procedimientos aprobados, instructivos técnicos y funcionales o flujos operativos que documenten cómo se implementa la firma electrónica avanzada en la organización.

8. Especificaciones técnicas, configuraciones del sistema, informes de pruebas o manuales del proveedor que evidencien que los sistemas soportan el uso de dispositivos criptográficos dedicados (como tokens o HSM) en todos los casos de uso requeridos.
9. Capturas de pantallas, manuales de usuario, informes de pruebas funcionales o documentación técnica que evidencien que la firma electrónica avanzada se encuentra integrada en los sistemas institucionales, permitiendo a los usuarios firmar o validar documentos directamente dentro del flujo de cada proceso.
10. Configuraciones del sistema, ejemplos de firmas con sellado, certificados de servidores TSA o reportes técnicos que evidencien que se utilizan sellos de tiempo compatibles con la especificación RFC 3161.
11. Informes de auditoría, pruebas de cumplimiento técnico, resultados de revisión o listas de verificación que permitan confirmar que se han auditado los módulos de firma, incluyendo aspectos como protocolos, formatos, manejo de claves y uso de sellado de tiempo.
12. Planes de mejora, actas de revisión, correos de comunicación o presentaciones institucionales que evidencien que los resultados de las auditorías fueron analizados y utilizados para la mejora continua de la solución, y comunicados formalmente al RSI.

Requisito CA.5 - Segregación de funciones en el acceso lógico

1. Configuraciones de flujo de autorizaciones, matrices de control de funciones, registros de tickets o procedimientos que evidencien que no es posible que un mismo usuario solicite, apruebe y asigne accesos en sistemas críticos.
2. Tickets de acceso, flujos de aprobación, configuraciones de sistema o planillas de control que permitan verificar que quien ejecuta la asignación de privilegios es distinto al que la aprueba.

3. Controles técnicos en herramientas de gestión, matrices de segregación, formularios de aprobación excepcional o reportes de revisión que evidencien que se impide la asignación conjunta de roles en conflicto salvo justificación formal.
4. Listados de usuarios con privilegios, criterios de asignación documentados, reportes de revisión de cuentas o configuraciones de sistemas que permitan verificar que se limita la cantidad de usuarios con privilegios administrativos conforme a lineamientos establecidos.
5. Diagramas de roles por entorno, configuraciones de herramientas, tickets de justificación o registros de revisión que evidencien que no se permite operar en múltiples entornos salvo justificación formal y documentada.
6. Manuales de funciones, matrices de segregación, actas de asignación de roles o evidencia organizacional que confirme que el personal que administra accesos no realiza auditoría sobre los mismos.
7. Matrices de incompatibilidades, instructivos internos, configuraciones de sistemas o planillas de revisión que permitan verificar que los conflictos entre roles o combinaciones de privilegios están identificados, documentados y gestionados.
8. Políticas internas, criterios documentados, formularios de aprobación o publicaciones oficiales donde se especifiquen las condiciones bajo las cuales se pueden autorizar privilegios administrativos.
9. Documentación de seguridad, lineamientos operativos, instructivos aprobados o actas que definan y justifiquen cuántos usuarios con privilegios de administrador deben existir por sistema o entorno.
10. Procedimiento de control de acceso lógico vigente que incluya una sección específica sobre la segregación de funciones, disponible en sistemas internos, manuales de seguridad o plataformas de documentación institucional.
11. Informes de auditoría, listas de verificación, reportes de revisión o actas de control que evidencien que se audita periódicamente el cumplimiento del procedimiento de segregación de funciones.

12. Informes de hallazgos, tickets de corrección, planes de acción o registros de seguimiento con responsables asignados que permitan constatar que las desviaciones identificadas se documentan y se gestionan adecuadamente.

Requisito CA.6 - Gestión de accesos y permisos

1. Formularios de solicitud de acceso, tickets aprobados, registros en sistemas de gestión o planillas firmadas por responsables que evidencien que los derechos de acceso se otorgan solo tras una autorización explícita.
2. Inventarios de dispositivos, formularios de asignación, tickets de aprobación, registros de configuración o controles de acceso que evidencien que los dispositivos externos utilizados por el personal están identificados, tienen un responsable asignado y su uso está autorizado.
3. Tickets aprobados, planillas de control, registros del sistema de gestión de identidades o archivos históricos que permitan verificar que toda autorización de acceso queda documentada.
4. Configuraciones del sistema, reportes técnicos, capturas de autenticación o instructivos de seguridad que permitan constatar que el acceso a activos críticos requiere autenticación con múltiple factor (MFA).
5. Configuraciones de permisos, matrices de roles, instructivos de asignación o reportes de revisión de accesos que evidencien que los accesos son otorgados según el mínimo nivel necesario para desempeñar la función asignada.
6. Procedimiento operativo aprobado y vigente, instructivo interno o diagrama de flujo que detalle los pasos para acceder a redes, sistemas o recursos de información de forma controlada.
7. Documento formal de política aprobado y difundido institucionalmente, que establezca criterios, responsabilidades y restricciones para el acceso lógico a los activos de información.

8. Informes de análisis de riesgo, matrices de amenazas, configuraciones de seguridad o documentación técnica que evidencien que los controles de acceso fueron definidos en función del nivel de riesgo asociado a los activos protegidos.
9. Secciones específicas de la política de acceso lógico, anexos o cláusulas donde se regulen los accesos privilegiados, sus condiciones de uso y los mecanismos de control aplicados.
10. Listas de verificación, actas de revisión, informes de cumplimiento o evidencias de evaluación que reflejen que en los procedimientos de revisión continua de accesos consideran las políticas, normas y regulaciones sobre protección de datos y privacidad.

5.6 Seguridad física y del ambiente

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito SF.1 - Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de procesamiento de datos y áreas relacionadas.
1. Planos de seguridad, relevamientos internos, informes de riesgo o matrices de clasificación de áreas que permitan verificar que la organización ha identificado qué sectores requieren control de acceso físico. 2. Fotografías, configuraciones de sistemas de control, registros de ingreso o informes técnicos que evidencien la existencia de barreras físicas, cerraduras electrónicas, lectores biométricos u otros mecanismos de control en el centro de procesamiento de datos. 3. Formularios de solicitud, tickets de autorización, planillas de control o registros de sistemas que evidencien que el acceso al centro de procesamiento de datos es evaluado, aprobado y registrado.

4. Diagramas de distribución física, documentación de seguridad, planos con zonas delimitadas o informes de arquitectura que muestren cómo se definen y aplican los perímetros de seguridad en el centro de procesamiento de datos y otras áreas protegidas.
5. Registros de ingreso, configuraciones de sistemas de control de accesos, fotografías o listas de áreas protegidas con barreras físicas y tecnológicas implementadas.
6. Solicitudes de acceso, tickets con aprobación, planillas firmadas o registros electrónicos que evidencien que el ingreso a áreas seguras es evaluado, autorizado y documentado.
7. Bitácoras electrónicas, reportes exportados de sistemas de control de acceso, planillas manuales o logs automatizados que permitan verificar que se lleva un registro de todos los accesos físicos realizados.
8. Documento de política aprobado por la dirección o el CSI, publicado en medios internos o incorporado en el marco normativo de seguridad de la organización que establezca criterios para el control de acceso físico.
9. Logs de control de accesos, reportes de incidentes, tickets de verificación o informes posteriores al evento que permitan demostrar que los registros de ingreso a áreas protegidas son revisados ante alertas o eventos específicos.
10. Configuraciones de sistemas, capturas de pantallas, manuales de seguridad o instructivos que indiquen que las aplicaciones que manejan información sensible requieren reautenticación periódica, especialmente desde ubicaciones de riesgo.
11. Procedimiento formal aprobado, cronogramas de revisión, listas de verificación, informes de control o actas de seguimiento que evidencien que la organización ha establecido un proceso periódico para revisar los accesos al centro de procesamiento de datos y a las áreas seguras.
12. Informes de auditoría interna, listas de hallazgos, planes de acción o resultados de control que permitan verificar el cumplimiento de los procedimientos establecidos para el acceso físico.
13. Configuraciones de políticas, reglas de firewall, soluciones de acceso seguro, instructivos operativos o reportes de monitoreo que demuestren

que existen restricciones y controles sobre accesos desde ubicaciones externas a la organización.

Requisito SF.2 - Implementar controles ambientales en los centros de procesamiento de datos y áreas relacionadas.
1. Informes de evaluación de riesgos, matrices de riesgo, estudios de impacto ambiental o relevamientos de infraestructura que evidencien que se han identificado los riesgos ambientales que podrían afectar al centro de procesamiento de datos. 2. Fotografías, reportes técnicos, contratos de mantenimiento o documentación de las instalaciones que evidencien la existencia de medidas de control ambiental. 3. Certificados de instalación, registros de mantenimiento, informes de inspección o fichas técnicas que evidencien la instalación de sistemas de detección y extinción de incendios en el centro de procesamiento de datos y su mantenimiento periódico. 4. Capturas de pantallas, diagramas de arquitectura, reportes de herramientas o manuales operativos que permitan verificar que se utilizan soluciones automatizadas para monitorear condiciones ambientales en el centro de procesamiento de datos. 5. Fichas técnicas, fotografías del sistema, registros de operación, contratos de mantenimiento o reportes de monitoreo que demuestren que se cuenta con un sistema de climatización activo que regula la temperatura y la humedad. 6. Documento de política vigente que incluya medidas de protección ambiental para el equipamiento, aprobado por la dirección o el CSI y disponible en medios institucionales. 7. Procedimiento formal, flujos operativos, instructivos técnicos o manuales de operación que documenten cómo se monitorean los controles ambientales, incluyendo el uso de herramientas automatizadas.

8. Informes de revisión, registros de ajustes, tickets de mejora o minutas técnicas que evidencien que los controles ambientales se revisan periódicamente y se adaptan a condiciones climáticas o tecnológicas cambiantes.
9. Informes de control interno, listas de verificación, hallazgos de auditoría o reportes de seguimiento que permitan verificar que se evalúa el cumplimiento de la política y los procedimientos ambientales.
10. Registros de incidentes o fallos ambientales, informes de análisis, minutas de revisión o versiones ajustadas de procedimientos que evidencien que los resultados del monitoreo se utilizan para extraer lecciones aprendidas y mejorar los procedimientos.

Requisito SF.3 - Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.

1. Registros de revisión posterior a incidentes, logs de eventos críticos, tickets de soporte o alertas gestionadas manualmente que evidencien que se realiza monitoreo reactivo o no sistemático sobre los servicios más críticos.
2. Registros de eventos críticos, configuraciones del sistema de logs, capturas de consolas de monitoreo o archivos de historial exportados que evidencien que se almacenan los registros de fallas y alertas críticas para su posterior revisión y análisis.
3. Capturas de herramientas, reportes de monitoreo, configuración de alertas o registros de eventos que demuestren que los activos críticos están monitoreados automáticamente y generan alertas ante incidentes.
4. Fichas técnicas de equipos, manuales del fabricante, reportes del sistema o configuraciones habilitadas que muestren que los dispositivos monitorean condiciones como temperatura, energía o ventilación.

5. Configuraciones del sistema, listas de distribución, capturas de correo o registro de alertas por SMS que permitan verificar que se han definido y activado notificaciones para incidentes o condiciones de riesgo.
6. Reportes del sistema, capturas de herramientas de monitoreo, registros de eventos o configuraciones que demuestren que se generan alertas ante comportamientos anómalos que podrían escalar a incidentes.
7. Configuraciones de alertas avanzadas, paneles de monitoreo o registros de eventos clasificados como precursores de fallos, que permitan demostrar que el sistema anticipa condiciones de riesgo.
8. Procedimiento formal vigente que describa las actividades de monitoreo, el uso de herramientas automatizadas y los responsables involucrados, utilizado como base operativa por el área técnica.
9. Configuraciones del sistema, listas de alertas, registros históricos o capturas de eventos que evidencien que los cambios de entorno (temperatura, humedad, energía, etc.) generan alertas para los activos clave de la organización.
10. Diagrama de arquitectura, reportes de correlación, capturas de plataformas de monitoreo unificado o configuraciones de integración que evidencien que se cruzan datos de diversas fuentes para generar alertas tanto reactivas como preventivas.
11. Informes de control interno, listas de verificación, cronogramas de auditoría o hallazgos registrados que evidencien que se verifica el cumplimiento de los procedimientos de monitoreo definidos para el centro de procesamiento de datos.

Requisito SF.4 - Seguridad del equipamiento
1. Inventario de dispositivos con barreras, fotografías de cerraduras o tapas de seguridad, planillas de control físico o registros de instalación

de sensores que evidencien que los equipos con información sensible están protegidos contra manipulaciones no autorizadas.

2. Actas de recepción, registros firmados, fotografías de embalajes o listas de verificación de inspección que evidencien que se revisa el estado de los empaques y se documentan daños o alteraciones al recibir equipamiento nuevo.
3. Capturas de BIOS, listados de configuración, informes técnicos o fotografías de conectores bloqueados que permitan verificar que los puertos no necesarios (USB, serie, etc.) están deshabilitados en los dispositivos del centro de procesamiento de datos.
4. Fotografías de sellos aplicados, inventario de cintas con su código correspondiente, instructivos internos o actas de control que evidencien la implementación de mecanismos que permitan detectar accesos físicos no autorizados.
5. Configuraciones del sistema operativo, políticas de grupo, capturas de pantalla o informes técnicos que evidencien que los dispositivos están configurados para bloquearse automáticamente tras 15 minutos sin uso.
6. Configuraciones de seguridad, scripts aplicados, informes de cumplimiento o parámetros técnicos que permitan comprobar que los sistemas están programados para cerrar la sesión después de 30 minutos de inactividad.
7. Documento aprobado por la dirección y/o el CSI, políticas internas difundidas, anexos normativos o registros de capacitación que evidencien que existe una política con lineamientos sobre protección física, manipulación y operación segura del equipamiento.
8. Procedimiento formal vigente, flujos de notificación, plantillas de registro o informes de aplicación que evidencien cómo se responde a eventos de manipulación, incluyendo evaluación de integridad y acciones inmediatas.
9. Documento operativo aprobado, manual técnico, instructivo de seguridad o políticas específicas que describan configuraciones

preventivas y las acciones esperadas ante eventos como dejar un equipo desatendido.

10. Informes de auditoría interna, listas de verificación aplicadas, cronogramas ejecutados o hallazgos documentados que permitan constatar que se revisa periódicamente el cumplimiento de los procedimientos de seguridad del equipamiento.
11. Actas de revisiones periódicas, versiones actualizadas de procedimientos, análisis de incidentes o registros de ajustes implementados que evidencien que se realiza una revisión formal de las medidas de seguridad y se incorporan mejoras.

Requisito SF.5 - Establecer el mantenimiento de los componentes críticos.

1. Cronogramas de mantenimiento, tickets de trabajo, órdenes de servicio o procedimientos internos que permitan verificar que el área de tecnología realiza mantenimiento sobre los activos del centro de procesamiento de datos.
2. Formularios, tickets de autorización, actas de aprobación o registros de usuarios habilitados que evidencien que los accesos remotos a activos informáticos con fines de mantenimiento son aprobados formalmente.
3. Planes técnicos, cronogramas de intervención, instructivos operativos o fichas de mantenimiento que muestren que existen planes definidos para dependencias o componentes críticos del centro de procesamiento de datos.
4. Documentos de planificación anual, calendarios operativos, actas de revisión o cronogramas aprobados que evidencien que se ha definido un plan de mantenimiento a nivel anual.
5. Tickets, listas de usuarios autorizados, registros de ingreso o configuraciones de control de acceso que permitan verificar que el acceso para tareas de mantenimiento se gestiona y limita a personal autorizado.

6. Registros de aprobación, planillas firmadas, correos institucionales o tickets donde conste que el RSI gestiona y aprueba los accesos remotos en el marco del plan anual de mantenimiento.
7. Procedimiento aprobado, diagramas de flujo operativos, instructivos técnicos o modelos de órdenes de trabajo que evidencien que las tareas de mantenimiento siguen criterios formales de planificación, coordinación con las áreas operativas, validación de funcionamiento y comunicación de resultados.
8. Documento de política aprobado institucionalmente, que establezca criterios de mantenimiento para los equipos de la organización.
9. Informes de control interno, listas de verificación, cronogramas de auditoría o hallazgos registrados que evidencien que se verifica el cumplimiento de los procedimientos de mantenimiento definidos para el equipamiento.
10. Informes posteriores a la intervención, registros de incidentes durante mantenimiento, planillas de acciones correctivas o versiones actualizadas de procedimientos que evidencien que, tras desvíos o fallos, se analizan causas, se ajustan procesos y se incorporan aprendizajes.

5.7 Seguridad de las operaciones

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito SO.1 - Gestionar las vulnerabilidades técnicas.
1. Informes de versiones instaladas, registros de parches aplicados, reportes de herramientas de gestión de activos o tickets de actualización que evidencien que el software base y las aplicaciones críticas se encuentran actualizados sin vulnerabilidades críticas conocidas. 2. Listados de activos con restricciones tecnológicas que no pueden ser actualizados, planillas justificadas, informes de excepción o

documentación de controles alternativos aplicados (como aislamiento, monitoreo reforzado, limitación de accesos, etc.) que permitan verificar que estos casos están identificados y controlados.

3. Plan formal aprobado, cronogramas de aplicación de parches, matrices de planificación o publicaciones internas que permitan constatar que existe un enfoque documentado para gestionar vulnerabilidades y aplicar parches.
4. Correos electrónicos, registros de suscripción, herramientas de agregación de alertas, tickets de análisis o actas de reuniones que evidencien que se reciben y analizan notificaciones de vulnerabilidades relevantes provenientes del CERTuy u otros organismos.
5. Planillas de análisis, matrices de criticidad, reportes de escaneo, criterios definidos o tickets de tratamiento que evidencien que las vulnerabilidades detectadas son evaluadas y priorizadas según su impacto y exposición.
6. Procedimiento técnico vigente, aprobado y difundido internamente, que describa las actividades, plazos, responsables y mecanismos para la gestión y resolución de vulnerabilidades.
7. Manuales de funciones, matrices de roles, procedimientos con responsables asignados o actas de designación que permitan verificar que hay personas o áreas responsables específicamente de la gestión de vulnerabilidades.
8. Informes de escaneo, cronogramas de ejecución, logs de herramientas de análisis o tickets de cierre que permitan demostrar que se realizan escaneos de vulnerabilidades con una frecuencia mínima de seis meses.
9. Informes de revisión interna, listas de verificación, hallazgos de auditoría o registros de cumplimiento que evidencien que se evalúa periódicamente la aplicación del plan de gestión de vulnerabilidades.
10. Reportes finales, correos institucionales, presentaciones internas o actas de reunión que permitan verificar que los resultados de las revisiones fueron comunicados formalmente al RSI.

11. Registros de análisis de vulnerabilidades tratadas, minutas de revisión, reportes de cierre de ciclo o versiones actualizadas de procedimientos que evidencien que las lecciones aprendidas son formalmente registradas y utilizadas para mejorar la respuesta frente a vulnerabilidades similares en el futuro.

Requisito SO.2 - Gestionar formalmente los cambios.

1. Correos institucionales, publicaciones en intranet, actas de reuniones, notificaciones en herramientas de gestión o tickets cerrados que permitan verificar que se comunican los cambios tecnológicos a las partes interesadas.
2. Formularios de cambio, tickets de aprobación, actas internas o registros del sistema de gestión que evidencien que los cambios tecnológicos fueron previamente autorizados por los responsables de los activos involucrados.
3. Manuales técnicos, procedimientos de desarrollo, flujos de gestión de cambios o repositorios internos que permitan verificar que está definido un mecanismo de control de versiones para los productos de software utilizados por la organización.
4. Guías de configuración, instructivos de seguridad, plantillas de línea base o registros de aplicación de hardening que evidencien que se han establecido criterios de configuración segura y líneas base para los productos de software y sistemas utilizados.
5. Evidencias de pruebas en entornos de desarrollo o preproducción, planes de pruebas, tickets con resultados o capturas de ambiente que permitan verificar que los cambios en infraestructura crítica se validan antes de ser aplicados en producción.
6. Documento de política aprobado institucionalmente que regule la gestión de cambios tecnológicos y contemple explícitamente el tratamiento de cambios de emergencia.

7. Procedimiento formal vigente, instructivos operativos, diagramas de flujo o manuales internos que detallen cómo se gestionan los cambios tecnológicos desde la solicitud hasta su cierre.
8. Tickets, planillas, reportes del sistema o formularios de gestión de cambios que permitan verificar que cada cambio tiene un responsable asignado y una justificación documentada.
9. Capturas de pantalla, licencias activas, manuales de uso o registros de operación en herramientas específicas (como Redmine, Jira, entre otras) que evidencien que se utilizan sistemas de soporte para la gestión de cambios.
10. Informes de auditoría interna, listas de verificación, hallazgos documentados o registros de revisión que demuestren que se evalúa el cumplimiento del procedimiento de gestión de cambios.
11. Correos, actas, presentaciones institucionales o informes de control que evidencien que los resultados de las revisiones de cambios son comunicados al RSI y a las áreas afectadas o interesadas.
12. Tickets de corrección, planes de acción, minutas de seguimiento o documentación de mejora continua que permita verificar que, ante desviaciones detectadas en la gestión de cambios, se toman y documentan medidas correctivas.

Requisito SO.3 - Gestionar la capacidad de los servicios y recursos que se encuentran operativos.

1. Informes de monitoreo, métricas de rendimiento, reportes de utilización o análisis de disponibilidad que evidencien que la capacidad actual instalada permite mantener operativos los servicios críticos.
2. Tickets de soporte, registros técnicos, logs de eventos o minutas de intervención que permitan verificar que se toman acciones puntuales para restaurar la capacidad operativa ante incidentes de saturación.

3. Informes de planificación, actas de reuniones interáreas, solicitudes de capacidad o análisis de demanda que evidencien que se contemplan los requerimientos del negocio al dimensionar servicios críticos.
4. Tableros o dashboards de monitoreo, reportes automatizados, históricos de consumo de recursos o herramientas de observabilidad que permitan detectar tempranamente problemas de capacidad.
5. Procedimiento formal, manual operativo o diagrama de procesos aprobado institucionalmente que defina cómo se gestiona la capacidad tecnológica en la organización.
6. Matrices de asignación de funciones, manuales de rol, procedimientos con responsables identificados o resoluciones internas que evidencien quiénes son los encargados del proceso de gestión de capacidad.
7. Acuerdos de nivel de servicio vigentes, cláusulas técnicas, anexos de servicios o compromisos formales que incluyan criterios de capacidad tecnológica dentro de su definición o seguimiento.
8. Documento de planificación de capacidad aprobado y disponible, que incluya análisis actuales, proyecciones, riesgos identificados y acciones previstas para asegurar el desempeño futuro.
9. Procedimientos técnicos, modelos de dimensionamiento, metodologías documentadas o herramientas utilizadas que evidencien cómo se realiza la estimación de capacidad dentro del marco del plan de gestión de la capacidad.
10. Informes de actualización, versiones comparadas, actas de seguimiento o registros de revisión que permitan comprobar que el plan de capacidad es evaluado y ajustado regularmente.
11. Minutas de reuniones técnicas, planes de acción, análisis de brechas o reportes de evolución que documenten acciones concretas propuestas para mejorar el proceso de gestión de capacidad.

Requisito SO.4 - Definir entornos separados para desarrollo, pruebas y producción.

1. Diagramas de arquitectura, configuraciones de red, restricciones de acceso o documentación técnica que evidencien que el entorno de producción está efectivamente separado de los demás entornos.
2. Listado de entornos, fichas técnicas, configuraciones de infraestructura o documentación de arquitectura que permita comprobar que existen plataformas adecuadas e independientes para las etapas de desarrollo, prueba y producción.
3. Flujos de pasaje a producción, tickets de cambio, permisos de acceso o configuraciones de repositorios que evidencien que se aplican controles al momento de mover código, configuraciones o datos entre entornos.
4. Políticas internas, registros de anonimización o seudonimización, controles de acceso o autorizaciones excepcionales que permitan verificar que el uso de datos reales en entornos de prueba está restringido o debidamente controlado.
5. Documento de política vigente, aprobado por la dirección y difundido internamente, que establezca criterios formales para la separación lógica y física de entornos tecnológicos.
6. Procedimiento operativo aprobado, instructivos técnicos o manuales de gestión que detallen cómo se administran los distintos entornos y cómo se realiza el pasaje entre ellos.
7. Manuales de funciones, matrices de roles, asignaciones formales o procedimientos que identifiquen quiénes son los responsables de la gestión de entornos y del pasaje a producción.
8. Planillas de pruebas, registros del sistema, bitácoras técnicas o capturas de herramientas que evidencien que durante las pruebas se registra información del entorno utilizado, incluyendo configuración y características de los datos de prueba.
9. Informes de auditoría interna, listas de verificación, reportes de hallazgos o evidencias de control interno que permitan verificar el cumplimiento de la política de separación de entornos y sus procedimientos asociados.
10. Informes de revisión, tickets de seguimiento, planes de acción o minutas de reuniones que evidencien que los resultados de las auditorías o

controles son registrados y que se toman medidas correctivas cuando se detectan desvíos.

Requisito SO.5 - Controlar software malicioso.

1. Capturas de pantalla, reportes del sistema, inventarios de licencias o listados generados por la consola de administración que evidencien que todos los equipos del personal cuentan con protección antimalware instalada y activa.
2. Tickets de soporte, registros de intervención, correos técnicos o minutas informales que permitan verificar que la resolución de infecciones o problemas vinculados a malware se realiza.
3. Listados de servidores, reportes de instalación, capturas del sistema o registros del software de seguridad que evidencien que todos los servidores cuentan con soluciones antimalware activas.
4. Capturas de configuración, políticas aplicadas por consola central, reportes de escaneo o planillas de verificación que permitan constatar que se realizan chequeos periódicos en los equipos del personal.
5. Documento de política aprobado y difundido institucionalmente que establezca los lineamientos generales para la prevención, detección y tratamiento de software malicioso.
6. Procedimiento formal vigente que describa los pasos a seguir ante la detección de malware, incluyendo responsables, plazos y registros asociados.
7. Capturas de la consola central, registros de gestión, manuales de operación o reportes generados desde la plataforma que permitan verificar que la protección antimalware se gestiona de forma centralizada.
8. Informes de gestión de activos y licenciamiento que verifiquen la correspondencia entre la cantidad de dispositivos en uso y las licencias de software antimalware adquiridas y asignadas, garantizando que no existan equipos sin cobertura.

9. Listas de bloqueo, configuraciones de proxy, reportes de firewall o herramientas de filtrado web que evidencien que se han implementado controles para restringir el acceso a sitios maliciosos o no autorizados.
10. Configuraciones de seguridad en móviles, manuales de MDM, capturas de aplicaciones de protección y versiones de la política de manejo de software malicioso donde se incluya explícitamente la protección contra software malicioso en dispositivos móviles.
11. Procedimiento documentado, registros de escaneo, tickets de remediación o reportes técnicos que evidencien que se detectan equipos sin protección activa y se toman acciones correctivas para subsanar la situación.
12. Bases de datos, reportes estadísticos, gráficos de tendencias o informes periódicos que documenten las infecciones detectadas, su análisis y la incorporación de esas lecciones en acciones de mejora continua.

Requisito SO.6 - Respaldar la información y realizar pruebas de restauración periódicas.

1. Registros de tareas programadas, reportes de ejecución de respaldos, cronogramas de respaldo o bitácoras de ejecución que evidencien que se realizan respaldos periódicos de aplicaciones, bases de datos y máquinas virtuales del centro de procesamiento de datos.
2. Configuraciones de permisos, registros de acceso, ubicaciones físicas controladas, configuraciones de almacenamiento remoto o documentación técnica que evidencien que los respaldos se almacenan en lugares seguros y con acceso restringido.
3. Procedimientos internos, configuraciones de las herramientas de respaldo, instructivos operativos o políticas técnicas donde se establezca el grado (completo, incremental, diferencial) y el período de retención de los respaldos.

4. Reportes de prueba, registros de recuperación simulada, actas de ejercicios o tickets de verificación que demuestren que se realizan pruebas periódicas de recuperación a partir de respaldos.
5. Configuraciones de almacenamiento, fichas técnicas de dispositivos, reportes de retención protegida o evidencias de uso de tecnologías que impidan la modificación posterior.
6. Capturas de herramientas de respaldo, reportes de software de respaldo, configuraciones programadas o licencias activas que permitan verificar que se utilizan soluciones automatizadas para ejecutar respaldos.
7. Documento de política vigente y aprobado, publicado internamente, que establezca los lineamientos generales para la ejecución, retención, almacenamiento y verificación de respaldos.
8. Procedimientos técnicos detallados, manuales de recuperación, instructivos de ejecución de respaldos o versiones validadas de guías operativas que describan cómo se realizan y prueban los respaldos.
9. Versiones comparadas del procedimiento, registros de revisión, tickets de actualización o actas de reuniones que permitan verificar que el procedimiento se actualiza cuando cambian los sistemas, infraestructura o requerimientos del negocio.
10. Mapas de vinculación, anexos cruzados, referencias entre documentos o actas de coordinación que evidencien que la política y el procedimiento de respaldos están alineados con el plan de contingencia y el plan de recuperación de la organización.
11. Cronogramas de revisión, informes de evaluación, registros de actualización o control de versiones que demuestren que tanto la política como el procedimiento de respaldos se revisan de manera periódica.

Requisito SO.7 - Registrar y monitorear los eventos de los sistemas.
1. Configuraciones del sistema, capturas de herramientas de logging, manuales técnicos o reportes de validación que evidencien que todos los

sistemas definidos como críticos tienen habilitados los registros de auditoría y eventos.

2. Reportes de análisis de incidentes, matrices de impacto, registros de evaluación posteriores al evento o minutas técnicas que permitan verificar que se analiza el impacto de los eventos sobre sistemas o servicios críticos.
3. Manuales de funciones, asignación de turnos, matrices de roles o listas de responsables que evidencien que hay personal asignado para detectar eventos en sistemas base y dispositivos perimetrales.
4. Capturas de sistemas, diagramas de arquitectura, licencias activas o registros de operación que evidencien el uso de herramientas que centralizan los logs de distintos activos tecnológicos.
5. Configuraciones de permisos, controles de integridad, cifrado de registros o reportes de hardening que permitan verificar que los logs están protegidos contra accesos indebidos o alteraciones.
6. Documentación técnica, matrices de criticidad, planes de continuidad o configuraciones del sistema que evidencien que se han establecido valores umbral (por ejemplo, respuesta máxima tolerable, carga aceptable, latencia crítica) para activos relevantes.
7. Configuraciones de sistemas, políticas internas, ejemplos de alertas generadas o reportes de monitoreo que permitan verificar que los sistemas críticos emiten alertas conforme al apetito de riesgo definido por la organización.
8. Capturas de herramientas de monitoreo, logs de eventos generados automáticamente, scripts de detección o reportes configurados que evidencien que se generan alertas automáticas ante eventos como conexiones externas, instalaciones no autorizadas, etc.
9. Matrices de responsabilidades, manuales de funciones o procedimientos técnicos que indiquen qué áreas o perfiles participan en actividades de monitoreo, incluyendo aquellas gestionadas mediante herramientas automatizadas.

10. Políticas de seguridad, procedimientos de archivo, configuraciones del sistema o documentos técnicos que establezcan los tiempos de conservación y eliminación de registros de auditoría.
11. Configuraciones de sincronización, capturas del servicio NTP, registros de monitoreo o informes de revisión que permitan verificar que todos los sistemas tienen relojes sincronizados.
12. Políticas de privacidad, cláusulas en la política de auditoría, instructivos internos o restricciones de acceso que evidencien que se protegen los datos personales contenidos en los registros.
13. Documento de política vigente y aprobado que establezca lineamientos para el registro, tratamiento y revisión de eventos, incluyendo sistemas de red, WAF y configuraciones críticas.
14. Procedimientos operativos, flujos de revisión, instructivos técnicos o versiones controladas que describan cómo se auditan y registran los eventos.
15. Capturas de herramientas SIEM, informes de correlación, reportes de incidentes agrupados o diagramas de arquitectura que demuestren el uso de soluciones que integran múltiples fuentes para correlacionar eventos.
16. Procedimientos documentados con actividades específicas para la detección y monitoreo de eventos, incluyendo configuraciones de alertas, responsables y frecuencia de revisión.
17. Procedimientos formales donde consten los umbrales de alerta y los criterios de impacto, ya sea en anexos, secciones técnicas o plantillas utilizadas en el monitoreo.
18. Informes de simulacros, registros de pruebas de detección, minutas de validación o tickets de mejora que evidencien que el procedimiento de monitoreo se prueba regularmente.
19. Reportes de auditoría, registros de sesión, configuraciones de control de privilegios o herramientas de monitoreo que permitan revisar específicamente la actividad realizada por usuarios con privilegios elevados.

20. Configuraciones de respuesta automática, reglas definidas en SIEM/SOAR, scripts ejecutados ante incidentes o ejemplos de acciones generadas automáticamente ante eventos de seguridad.
21. Informes de auditoría, listas de verificación, actas de revisión o resultados documentados de controles internos que verifiquen el cumplimiento de la política y los procedimientos de monitoreo y auditoría.
22. Informes finales, actas de reunión, correos institucionales o presentaciones que evidencien que los resultados de las revisiones fueron compartidos con el RSI y otras partes relevantes de la organización.

Requisito SO.8 - Gestionar la instalación de software.

1. Instructivos internos, manuales de operación, procedimientos técnicos o publicaciones institucionales que establezcan las reglas y condiciones bajo las cuales se permite la instalación de software en los equipos de la organización.
2. Correos institucionales, registros de capacitación, publicaciones en intranet o actas de comunicación que evidencien que las pautas de instalación de software fueron comunicadas al personal.
3. Configuraciones de control de privilegios, políticas de grupo, registros de roles o tickets de solicitud que demuestren que únicamente los usuarios autorizados pueden instalar software en los equipos.
4. Configuraciones de sistemas operativos, manuales técnicos, controles de acceso o políticas internas que permitan verificar que existe una separación clara entre utilidades del sistema y software de aplicación, limitando el acceso a componentes críticos.
5. Listados de software admitido, actas de aprobación, versiones controladas o planillas firmadas que evidencien que existe una lista oficial de software autorizado y que esta ha sido revisada y aprobada por el RSI.

6. Informes de revisión, escaneos de inventario, herramientas de detección o reportes técnicos que evidencien que se realizan controles para verificar que el software instalado cumple con la lista autorizada.
7. Informes de control, correos institucionales, presentaciones o actas de reunión que demuestren que los resultados de las revisiones sobre software instalado fueron comunicados al RSI y a las áreas correspondientes.

5.8 Seguridad de las comunicaciones

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito SC.6 - Establecer acuerdos de no divulgación.

1. Copias firmadas de acuerdos de confidencialidad, registros en sistemas de gestión de contratos, tickets de alta o actas de firma que evidencien que los proveedores firman acuerdos de no divulgación antes del inicio de la relación comercial.
2. Contratos de ingreso, extractos del estatuto o normativa interna, formularios de acuse de recibo o registros de inducción que evidencien que todo nuevo personal queda formalmente alcanzado por compromisos de confidencialidad.
3. Contratos de trabajo, acuerdos marco, anexos legales, normativa interna o registros de firma que demuestren que la obligación de confidencialidad se extiende a todo el personal, sin excepción de rol ni tipo de contratación.
4. Acuerdos de confidencialidad firmados, planillas de control de documentos legales, cláusulas contractuales o actas de revisión que evidencien que los proveedores con acceso a información sensible tienen firmados los NDAs correspondientes.
5. Textos de acuerdos de no divulgación firmados, plantillas legales o cláusulas contractuales donde se detallen las consecuencias en caso de incumplimiento, así como las responsabilidades asumidas por el proveedor o el personal.

6. Cronogramas de revisión, informes de actualización, versiones comparadas o registros legales que evidencien que los acuerdos de confidencialidad son revisados de forma periódica para verificar su vigencia y aplicabilidad.
7. Informes de incidentes, tickets de reclamos, registros de sanciones o actas de evaluación que permitan verificar que se revisan los casos en que se detectan incumplimientos o desvíos respecto a lo establecido en los acuerdos de confidencialidad.
8. Correos institucionales, informes de seguimiento, minutas de reunión o presentaciones internas que evidencien que los resultados de las revisiones fueron comunicados al RSI y a otras partes interesadas relevantes.

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.

1. Capturas del navegador, reportes de escaneo de puertos o configuraciones del servidor que evidencien que el Webmail institucional solo es accesible mediante HTTPS y no permite conexiones HTTP.
2. Listas de control de acceso, reglas de firewall, configuraciones del servidor de correo, políticas institucionales o registros de monitoreo que permitan verificar que no se permite el acceso a cuentas institucionales desde servicios de Webmail externos.
3. Capturas de los certificados digitales del Webmail, reportes de validez (emitidos por CA confiables), configuraciones del servidor o documentación técnica que evidencien su vigencia y validez.
4. Configuraciones del servidor, escaneos de seguridad (por ejemplo, SSL Labs), archivos de configuración de TLS o reportes de revisión que evidencien que se han deshabilitado versiones inseguras de TLS/SSL.

5. Logs del servidor, reportes de monitoreo, actas de revisión o tickets que evidencien la verificación periódica de accesos indebidos desde Webmail externos no autorizados.
6. Política institucional o procedimiento de cifrado, capturas de configuración de S/MIME o PGP (entre otros), correos cifrados de ejemplo, instructivos o evidencia técnica que demuestren el uso de cifrado a nivel de mensaje para correos de alto riesgo.
7. Materiales de capacitación, manuales de uso seguro del Webmail, actas de talleres, correos de difusión o formularios de aceptación que evidencien la capacitación sobre uso seguro y restricciones de acceso externo.
8. Informes de auditoría, cronogramas de verificación, hallazgos documentados o registros de revisión de certificados y accesos que evidencien auditorías periódicas sobre el servicio de Webmail.
9. Resultados de pruebas técnicas (penetration testing, SSL Labs, escaneos de configuración, etc.), registros de validación o informes de seguridad que demuestren la efectividad del cifrado y de la configuración segura del Webmail.

Requisito SC.13 - Debe existir segregación a nivel de servicios de información.

1. Diagramas de red, configuraciones de firewall, reglas de ruteo o informes técnicos que evidencien que la red se encuentra segmentada al menos entre zonas expuestas (como Internet) y redes privadas de la organización.
2. Planillas técnicas, diagramas de red, listados de servicios o configuraciones exportadas que evidencien que la organización ha identificado y documentado los principales servicios de red que utiliza.

3. Listados de interconexiones, diagramas de red, registros de enlaces, contratos de conectividad o actas técnicas que permitan verificar que se mantiene un inventario actualizado de las interconexiones con otras entidades.
4. Informes de diseño de red, justificaciones técnicas, configuraciones de VLANs, segmentación por servicios o criticidad que evidencien que la red está organizada en función de criterios específicos de la organización.
5. Reglas de firewall, listas de control de acceso (ACL), configuraciones de seguridad o documentación de red que permitan comprobar que se ha definido y aplicado una postura por defecto (por ejemplo, denegar por defecto y permitir explícitamente) en la comunicación entre segmentos.
6. Acuerdos de seguridad de interconexión, contratos con anexos técnicos, formularios de evaluación de riesgo, fichas de interconexión aprobadas o actas de aprobación que evidencien que cada conexión con terceros está formalmente autorizada, describe interfaz, datos intercambiados y requisitos de seguridad.
7. Contratos vigentes, acuerdos de nivel de servicio (SLA), anexos de seguridad o cláusulas contractuales que evidencien que los proveedores de servicios de red están sujetos a condiciones formales que incluyen compromisos de seguridad.
8. Documento de política aprobado por la Dirección y/o el CSI, versiones controladas, actas de difusión interna o registros de capacitación que permitan verificar que existe una política de seguridad de las comunicaciones.
9. Diagramas técnicos, planos de arquitectura de red, capturas de plataformas de monitoreo o documentos validados que permitan verificar que la organización mantiene un diagrama de red actualizado.
10. Reportes de monitoreo, capturas de herramientas de análisis, logs de tráfico o estudios de uso que evidencien que se conoce, analiza y revisa periódicamente el comportamiento del tráfico entre los distintos segmentos.
11. Configuraciones de firewall, registros de inspección profunda de paquetes, túneles cifrados, reglas de acceso o registros técnicos que

evidencien que las comunicaciones entrantes y salientes entre segmentos están protegidas adecuadamente.

12. Informes de auditoría interna, listas de verificación aplicadas, hallazgos documentados o cronogramas de revisión que evidencien que se realiza control interno periódico sobre el cumplimiento de la segregación definida y la vigencia de los acuerdos de interconexión autorizados.

Requisito SC.14 - Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.

1. Configuraciones de cifrado en protocolos de red, certificados digitales instalados, configuraciones de VPN o reportes técnicos que evidencien que se implementan controles criptográficos para proteger los datos que circulan entre sistemas.
2. Capturas de uso de HTTPS, SFTP, TLS, VPN o herramientas seguras de transferencia, junto con procedimientos técnicos o instructivos que evidencien que la transmisión de información sensible o confidencial se realiza mediante canales seguros.
3. Políticas técnicas, procedimientos de desarrollo, documentación de arquitectura o listas de tecnologías permitidas que evidencien que se aplica un conjunto reducido y consistente de tecnologías criptográficas en todos los sistemas y aplicaciones.
4. Procedimientos documentados, instructivos operativos o diagramas de flujo que establezcan cómo debe realizarse la transferencia segura de información tanto física como electrónica.
5. Contratos, convenios, NDA o cláusulas específicas en acuerdos que establezcan responsabilidades, controles criptográficos y medidas de seguridad en la transferencia de información con terceros.
6. Procedimientos de clasificación, matrices de tratamiento, configuraciones de sistemas o anexos en políticas que evidencien que las medidas aplicadas en la transferencia varían en función del nivel de sensibilidad de los datos.

7. Informes de revisión, análisis de configuraciones, pruebas de cumplimiento técnico o planes de mejora que permitan comprobar que se evalúan periódicamente los controles criptográficos aplicados a la protección de datos en tránsito.

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).

1. Planillas de control, registros internos, documentación de arquitectura, catálogos de sistemas o reportes generados por herramientas de descubrimiento que evidencien que la organización mantiene un inventario actualizado de todos sus sitios web institucionales.
2. Capturas de configuración del WAF, reportes de actividad, registros de eventos o documentación técnica que permitan verificar que todas las aplicaciones web expuestas en Internet cuentan con un WAF configurado al menos en modo detección.
3. Configuraciones del WAF, registros de bloqueos, reportes de eventos o políticas aplicadas que evidencien que el WAF en producción ha evolucionado desde el modo detección hacia el modo bloqueo efectivo.
4. Capturas del entorno de pruebas, diagramas de arquitectura, registros de instalación o informes de validación que permitan constatar que se cuenta con un WAF activo en el ambiente de testing para realizar pruebas funcionales antes del despliegue.
5. Tickets de implementación, planillas de cambios, reportes de pruebas y versiones aprobadas que evidencien que las reglas del WAF se impactan en producción únicamente después de ser validadas en el entorno de pruebas.
6. Diagramas de integración, capturas de la consola de monitoreo, reportes centralizados o configuraciones de reenvío de logs que permitan verificar que los registros del WAF se consolidan en una plataforma de monitoreo central.

7. Configuraciones de alertas automáticas, paneles de análisis, scripts de revisión o reportes generados automáticamente que demuestren que el análisis de los registros del WAF incorpora mecanismos automatizados que facilitan la revisión de eventos.

5.9 Adquisición, desarrollo y mantenimiento de los sistemas

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito AD.1 - Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.

1. Documentación metodológica, plantillas de planificación, cronogramas, manuales de gestión o documentos de alcance que evidencien que se utilizan lineamientos generales de desarrollo de sistemas incluyendo principios básicos de gestión de proyectos.
2. Instructivos de codificación segura, políticas técnicas, documentación de arquitectura o revisión de requisitos funcionales que demuestren que los proyectos de desarrollo integran principios de seguridad desde etapas tempranas.
3. Repositorios de código con historial de versiones, evidencias de revisiones (pull requests, merge requests), logs de control de cambios o capturas de herramientas que evidencien que se aplica control de versiones y revisión de código sistemática.
4. Planes de prueba, resultados de pruebas, casos de prueba con enfoque en seguridad o herramientas utilizadas que evidencien que las actividades de testing están sistematizadas e incluyen validaciones de seguridad.
5. Procedimiento técnico aprobado, instructivos operativos, flujos documentados o manuales internos que describan cómo se realizan las pruebas de seguridad en los desarrollos, incluyendo herramientas y responsabilidades.

6. Listas de verificación, criterios documentados, actas de validación o plantillas de cierre de proyecto que evidencien que la aceptación de los productos incluye criterios específicos de seguridad de la información.
7. Contratos con cláusulas de seguridad, anexos técnicos, requisitos mínimos documentados o plantillas de adquisición que evidencien que los proveedores deben cumplir con lineamientos de desarrollo seguro definidos por la organización.
8. Informes de revisión, listas de verificación internas, hallazgos documentados o auditorías que demuestren que se realiza control interno sobre el cumplimiento de los métodos y procedimientos de seguridad establecidos para el desarrollo.
9. Informes de control, actas de comité, correos institucionales o presentaciones que permitan verificar que los resultados de las actividades de control fueron comunicados formalmente al RSI y demás partes interesadas.
10. Planes de acción, registros de incidentes, tickets de remediación o evidencias de aplicación de medidas que evidencien que se toman acciones correctivas ante desviaciones detectadas en proyectos de desarrollo o adquisición.

Requisito AD.2 - Incluir requisitos de seguridad de la información para la adquisición de productos y servicios de tecnología.

1. Políticas institucionales, resoluciones aprobadas, instructivos de compra o documentos normativos que evidencien que existen criterios definidos para la adquisición de sistemas y servicios tecnológicos, incluyendo consideraciones de seguridad.
2. Solicitudes de cotización, pliegos de licitación, formularios de evaluación de ofertas o plantillas de requerimientos técnicos que permitan verificar que se incorporan requisitos específicos de seguridad en los procesos de compra.

3. Cuadros comparativos, informes de análisis de proveedores, actas de evaluación técnica o listas de verificación de cumplimiento que evidencien que antes de la contratación se analizó la capacidad del proveedor para cumplir con los requisitos de seguridad definidos.
4. Actas de aceptación, reportes de validación técnica, resultados de pruebas, revisiones documentales o planillas de conformidad que evidencien que los entregables fueron revisados y aprobados en función de los criterios de seguridad establecidos.
5. Contratos firmados, anexos técnicos, cláusulas contractuales o acuerdos de nivel de servicio que permitan verificar que el proveedor se compromete a mantener actualizaciones, aplicar parches de seguridad y gestionar incidentes, entre otras medidas, durante la vigencia del producto o servicio.
6. Actas de cierre de proyectos, informes posteriores al cierre del proyecto, recomendaciones de auditoría, planillas de mejora continua o registros de retroalimentación que evidencien que se incorporan aprendizajes de experiencias anteriores y auditorías en la definición de futuros requisitos de seguridad en adquisiciones.

5.10 Relación con proveedores

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito RP.1 - Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.

1. Listados de proveedores críticos, matrices de clasificación de proveedores, registros de puntos de contacto operativos, contratos con responsables designados o capturas del sistema de gestión de compras que permitan verificar que cada proveedor tiene un referente operativo identificado.
2. Copias de SLAs firmados, tickets de gestión contractual, reportes de cumplimiento de niveles de servicio, planillas de revisión de SLA o actas

de negociación que permitan constatar que los proveedores críticos cuentan con acuerdos firmados con metas de servicio definidas.

3. Matrices de riesgo de terceros, planillas de evaluación de proveedores, listas de verificación de revisión de antecedentes, reportes de seguimiento o flujos de aprobación que evidencien que existen mecanismos formales para identificar y gestionar riesgos vinculados a proveedores de servicios críticos.
4. Contratos firmados con cláusulas específicas, extractos contractuales, reportes de auditoría contractual, validaciones legales o plantillas de contrato que evidencien que se obliga a los proveedores a notificar incidentes confirmados o sospechados de forma oportuna.
5. Contratos vigentes, plantillas de términos y condiciones, actas de aprobación legal, cláusulas de confidencialidad y seguridad o reportes de revisión contractual que permitan verificar que los proveedores críticos tienen responsabilidades explícitas sobre la protección de la información.
6. Documento de política vigente y aprobado que establezca los criterios, roles y lineamientos para la selección, vinculación, seguimiento y desvinculación de proveedores, con énfasis en aquellos que impactan activos y servicios críticos.
7. Procedimientos documentados, diagramas de flujo de procesos, formularios usados en cada etapa, registros de aplicación del procedimiento o herramientas de seguimiento que permitan confirmar que se gestiona el ciclo completo del proveedor (selección, contratación, seguimiento y finalización).
8. Registros de evaluación previa a la contratación, planes de seguimiento durante la prestación, auditorías periódicas a proveedores, planes de salida o revisión de continuidad que evidencien que la gestión de riesgos se aplica desde la adquisición hasta el fin del vínculo.

Requisito RP.2 - Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.

1. Pliegos de compra, formularios de requerimiento, lista de verificación de evaluación técnica, condiciones contractuales estándar o capturas del sistema de compras que evidencien que las adquisiciones de soluciones o servicios incluyen requisitos mínimos de seguridad de la información.
2. Listados de KPIs definidos, tableros o dashboards de seguimiento, reportes de desempeño o planillas de control que permitan verificar que se han establecido métricas para evaluar la gestión y seguridad de los proveedores.
3. Extractos de contratos, plantillas legales, minutas de negociación, tickets de revisión o validaciones jurídicas que evidencien que los acuerdos con proveedores críticos contemplan cláusulas de ajuste ante cambios en el servicio, tecnología o normativa aplicable.
4. Calendarios anuales de evaluación, cronogramas aprobados, matrices de seguimiento o procedimientos internos que permitan confirmar que existe una periodicidad definida para evaluar a los proveedores.
5. Informes de evaluación de desempeño, actas de revisión de proveedores, reportes de cumplimiento de requisitos o formularios de evaluación con criterios de seguridad que permitan verificar que se registran los resultados de las evaluaciones de desempeño de forma estructurada.
6. Bitácoras de incumplimientos, tickets de incidentes relacionados a proveedores, actas de reuniones de seguimiento, planes de mejora o evidencias de penalizaciones que evidencien que los desvíos contractuales se documentan y gestionan adecuadamente.
7. Actas de revisión contractual, informes de adecuación, tickets de actualización de contratos o matrices de cambios normativos que permitan constatar que los contratos son revisados regularmente para mantener su alineación con las necesidades actuales.
8. Matrices de evaluación de proveedores basadas en criticidad, reportes de clasificación de riesgos, flujos de aprobación o criterios de selección que evidencien que se evalúa a los proveedores en función del impacto en el negocio y el riesgo asociado al servicio.
9. Registros de decisiones de compra basadas en evaluaciones anteriores, tickets de actualización de condiciones contractuales, minutas de comité de

compras o comparativas históricas de desempeño que permitan verificar que los resultados de evaluación inciden en futuras contrataciones o renovaciones.

5.11 Gestión de incidentes

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito GI.1 - Planificar la gestión de los incidentes de seguridad de la información.
1. Listados oficiales de contactos, configuraciones del sistema de tickets, capturas de formularios de reporte o actas de comunicación interna que evidencien quiénes son los puntos de contacto habilitados para la recepción de eventos de seguridad. 2. Planillas de contacto de actores clave, directorios de emergencias, bases de datos internas, anexos al plan de gestión de incidentes o extractos de herramientas de respuesta que permitan verificar que están identificadas y registradas las personas y entidades relevantes ante un incidente. 3. Capturas de sistemas de tickets, plataformas de monitoreo, consolas de SIEM, herramientas de análisis forense o documentación técnica de las soluciones utilizadas que permitan constatar que se cuenta con herramientas tecnológicas para apoyar la gestión de incidentes. 4. Procedimiento aprobado, diagramas de flujo, fichas por etapa o manuales operativos que detallen las fases de detección, registro, análisis, contención, erradicación y cierre, y que permitan verificar que hay una guía estructurada para abordar incidentes. 5. Documento de política vigente y aprobado que establezca los lineamientos institucionales para la gestión de incidentes de seguridad, incluyendo su alcance, objetivos, roles y principios rectores.

6. Registros de capacitación, correos institucionales, logs de accesos a intranet, actas de talleres o evidencias de envío que permitan confirmar que la política de gestión de incidentes fue comunicada a las partes interesadas.
7. Informes de auditoría, cronogramas ejecutados, hallazgos documentados o registros de actividades de verificación que evidencien que se realizan auditorías internas sobre cumplimiento de la política y procedimientos de gestión de incidentes.
8. Actas de comunicación al RSI, informes de seguimiento, planes de acción o tickets de remediación que permitan verificar que se informan los resultados de auditoría y se actúa sobre los desvíos detectados.

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.

1. Tickets de escalamiento, registros de correo, actas de reunión, protocolos de notificación o logs del sistema de gestión que evidencien que los eventos anómalos son informados a personas con capacidad de articular respuestas.
2. Lineamientos aprobados, anexos a políticas o procedimientos, tablas de categorización, instructivos operativos o formatos utilizados que permitan verificar que existe una forma definida para clasificar los incidentes por tipo y criticidad.
3. Procedimiento documentado, criterios en el sistema de tickets, manuales de respuesta o actas de capacitación que permitan constatar que existe una lógica definida para identificar cuándo múltiples eventos conforman un incidente.
4. Procedimientos internos, criterios legales incorporados en el plan de respuesta, ejemplos documentados, referencias a la Ley 20.327 o actas de consulta con asesores jurídicos que evidencien que la organización ha definido cómo identificar cuándo un evento de seguridad debe ser

clasificado como posible delito y canalizado conforme a la normativa aplicable.

5. Matrices de severidad, registros de clasificación, ejemplos documentados, formularios de incidentes o configuraciones de herramientas que evidencien el uso de una escala estructurada para clasificar los incidentes.
6. Procedimientos operativos, tablas de respuesta, instructivos por nivel de severidad o configuraciones de SLA en sistemas que permitan verificar que existen tiempos y acciones predefinidas para cada categoría de incidente.
7. Documento de procedimiento vigente, plantillas de análisis de impacto, registros de aplicación en incidentes anteriores o reportes forenses que evidencien que el análisis de impacto forma parte integral de la gestión de incidentes.
8. Secciones del procedimiento donde se detallen criterios de escalamiento, matrices de decisión, diagramas de flujo o registros de escalamiento que permitan verificar la existencia de reglas claras basadas en activos, criticidad y severidad.
9. Capturas de consolas de SIEM, sistemas de tickets, logs de ingreso de incidentes o documentación de herramientas utilizadas que evidencien que se cuenta con soporte automatizado coherente con el procedimiento definido.
10. Matriz de categorías vs. acciones, procedimientos técnicos, playbooks operativos o configuraciones del sistema de respuesta que permitan constatar que las acciones definidas están alineadas al plan de respuesta institucional.
11. Actas de revisión, versiones históricas de las escalas, análisis de cambios, informes de adecuación o reportes de tendencias que evidencien que se revisan periódicamente las categorías considerando cambios en amenazas o en el negocio.
12. Reportes estadísticos, tableros o dashboards, gráficos mensuales, entregables del área de seguridad o registros de reuniones que permitan verificar el uso de datos históricos categorizados.
13. Planes de mejora, registros de revisión de controles, análisis posterior al incidente, evidencia de implementación de medidas preventivas o

comparativas de control que evidencien que las estadísticas se usan para fortalecer la postura de seguridad.

Requisito GI.3 - Informar de forma completa e inmediata a las partes interesadas .
1. Registros de notificación, correos enviados, tickets de coordinación, extractos del procedimiento o actas de respuesta que evidencien que los reportes se realizan conforme a los criterios del equipo de respuesta correspondiente (CERTuy, otro externo o interno). 2. Registros de notificación a la URCDP, correos institucionales, tickets cerrados, copias de formularios enviados o actas internas que permitan constatar que se informa conforme a la normativa vigente en casos que involucran datos personales. 3. Registros de denuncias realizadas, correos institucionales con documentación adjunta, actas de decisión o comunicaciones formales con asesoría legal que evidencien que la organización canaliza ante la Unidad de Cibercrimen del Ministerio del Interior aquellos incidentes que pueden constituir un delito según la normativa vigente. 4. Planillas de registro, entradas en el sistema de gestión de incidentes, capturas de logs de notificación o historiales de mensajes que evidencien las comunicaciones efectuadas, con detalle de hora, contenido y destinatario. 5. Documento vigente aprobado que defina cómo, cuándo y a quién se comunica un incidente, incluyendo flujos, responsabilidades y medios de contacto habilitados. 6. Actas de revisión, versiones anteriores del procedimiento, informes de cambios normativos o recomendaciones del CERTuy que permitan verificar que el procedimiento es actualizado regularmente.

7. Cronogramas de simulacros, informes de ejecución, registros de tiempos de respuesta, capturas del sistema o reportes de evaluación que evidencien que se realizaron pruebas para validar la eficacia del canal de reporte.
8. Informes de auditoría interna o externa, hallazgos documentados, recomendaciones implementadas o cronogramas ejecutados que permitan constatar que se auditan los mecanismos de notificación de incidentes.

Requisito GI.4 - Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.

1. Tickets de incidentes, formularios de notificación, registros de aplicación del procedimiento, capturas del sistema o reportes de eventos que permitan verificar que los incidentes se reportan conforme a pautas definidas por la organización.
2. Registros de asistencia, materiales de formación, encuestas de comprensión, logs de acceso a manuales o actas de sesiones informativas que evidencien que el personal fue instruido en cómo reportar incidentes de seguridad.
3. Entradas en el sistema de gestión de incidentes, planillas de registro, historiales de incidentes o capturas de herramientas que permitan constatar que todos los incidentes son registrados.
4. Historias de incidente, auditorías del ciclo de vida del incidente, gráficos de línea de tiempo o reportes exportados desde la herramienta de gestión que evidencien la trazabilidad desde la detección hasta el cierre.
5. Procedimiento aprobado, plantilla de registro o campos en la herramienta utilizados para documentar fecha, tipo de incidente, activos afectados, estado y demás información relevante.
6. Capturas de sistemas como SIEM, consolas de monitoreo, plataformas de tickets o logs de automatización que permitan verificar que el reporte y registro se realiza mediante herramientas automatizadas.

7. Informes de verificación interna, listas de verificación de cumplimiento, reportes de auditoría cruzada o matrices de control que permitan constatar que se revisa el cumplimiento del procedimiento de reporte.
8. Versiones actualizadas del procedimiento, actas de revisión, acciones correctivas documentadas o tickets de mejora que evidencien que los resultados de las actividades de control se utilizan para ajustar el procedimiento.

Requisito GI.5 - Responder ante incidentes de seguridad de la información.

1. Diagramas de flujo de respuesta, protocolos operativos, instructivos técnicos o anexos del procedimiento que evidencien los mecanismos definidos para responder ante incidentes.
2. Registros de incidentes atendidos, tickets de contención, reportes posteriores al incidente o bitácoras de acciones ejecutadas que permitan verificar que se actúa para mitigar consecuencias.
3. Informes forenses, actas de solicitud de análisis, capturas de herramientas especializadas o bitácoras de intervención que evidencien la realización de análisis forense ante incidentes relevantes.
4. Procedimiento de preservación de evidencias, instructivos de cadena de custodia, formularios utilizados o anexos forenses que permitan constatar que se define cómo garantizar la integridad de la evidencia.
5. Listados de acciones de contención por tipo de incidente, plantillas de respuesta inmediata, registros de activación de contención o instructivos de mitigación que evidencien cómo se reduce el impacto en el entorno operativo.
6. Planes de remediación documentados, reportes de tareas posteriores al incidente, evidencias de aplicación de medidas correctivas o matrices de acciones que permitan verificar la existencia de planes específicos de remediación.

7. Documento formal y vigente que describa fases, roles, actividades y responsabilidades de la respuesta ante incidentes de seguridad de la información.
8. Manuales, procedimientos o guías técnicas específicas que regulen la ejecución de análisis forense digital en la organización.
9. Designación formal, descripción de roles, organigrama, acta de asignación o referencias explícitas en el plan que permitan identificar claramente al responsable designado.
10. Política de gestión de incidentes que incluya la revisión de la estrategia de respuesta, instructivo para actualización periódica, plantillas de evaluación de efectividad o criterios documentados que permitan verificar que existe una línea base de revisión estratégica de gestión de incidentes.
11. Actas de revisión, cronogramas ejecutados, listas de procesos evaluados o informes de adecuación que evidencien que se revisan regularmente los procesos que afectan servicios críticos.
12. Informes de incidentes enviados a la dirección, correos electrónicos institucionales con adjuntos o registros de envío, actas de reunión donde se haya discutido el incidente, tickets o registros de escalamiento con destinatarios identificados, o registros del sistema de gestión de incidentes que indiquen su derivación a niveles directivos.
13. Cronograma de pruebas, informes de simulacros, resultados de ejercicios de respuesta o registros de participación que permitan verificar que el plan se prueba al menos una vez al año.
14. Informes de incidentes entregados, actas de comité, registros de comunicaciones que evidencien que los principales responsables reciben información periódica sobre incidentes.
15. Informes de auditoría interna, listas de chequeo, hallazgos registrados o planes de mejora derivados que evidencien que se audita el cumplimiento del plan o procedimiento de respuesta.
16. Versiones revisadas del plan, matrices de cambios, actas de revisión o evidencia de incorporación de lecciones aprendidas que permitan constatar que las mejoras detectadas se integran en la estrategia.

17. Tableros o dashboards, reportes de KPIs, métricas operativas o entregables de gestión que permitan verificar que se generan y utilizan indicadores para el control de la respuesta a incidentes.

Requisito GI.6 - Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.

1. Registros posteriores al incidente, actas de reuniones técnicas, formularios de análisis retrospectivo o matrices de causas raíz que evidencien que se identifican, registran y analizan lecciones aprendidas específicamente de incidentes vinculados al centro de procesamiento de datos.
2. Reportes consolidados, análisis centralizados de incidentes, actas del comité de seguridad, planillas compartidas o herramientas de gestión que permitan constatar que se capturan y analizan lecciones aprendidas de incidentes en toda la organización.
3. Correos de difusión, informes ejecutivos, presentaciones institucionales, minutas de reuniones interáreas o publicaciones internas que evidencien que las lecciones aprendidas son compartidas con los actores relevantes.
4. Capturas de sistemas de gestión, funcionalidades específicas en plataformas de tickets, bases de datos internas o formularios digitales que permitan verificar que se utilizan herramientas específicas para registrar y dar seguimiento a las lecciones aprendidas.
5. Versiones actualizadas de planes de respuesta, anexos de mejoras, evidencias de revisión periódica o decisiones justificadas con base en aprendizajes previos que demuestren que se ajustan los planes ante hallazgos posteriores a los incidentes.
6. Cambios implementados en diagramas de comunicación, ajustes en matrices de escalamiento, actas de decisiones técnicas o comparativas antes/después de procesos modificados que permitan verificar que las lecciones impactan en la mejora operativa.
7. Planes de mejora institucionales, evidencia de rediseño de procesos, solicitudes de cambio aprobadas o reportes de reingeniería que evidencien

que las lecciones se utilizan más allá del área de seguridad, mejorando procesos de la organización.

8. Tableros o dashboards de seguimiento, reportes de cumplimiento, métricas sobre cierre de hallazgos o visualizaciones internas que permitan constatar que se generan indicadores sobre el tratamiento de lecciones aprendidas.
9. KPIs asociados a controles modificados, análisis de recurrencia de incidentes, reportes de mejora continua o evidencia de indicadores diseñados para evaluar la efectividad de las acciones correctivas implementadas.

5.12 Continuidad de las operaciones

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito CO.1 - Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de procesamiento de datos.

1. Planos eléctricos del centro de procesamiento de datos, registros de instalación, fotografías de los equipos, fichas técnicas de UPS instaladas o reportes de mantenimiento que permitan verificar la existencia de redundancia en la alimentación eléctrica.
2. Diagramas de infraestructura, contratos de instalación, reportes técnicos o documentación de proveedores que evidencien que el centro de procesamiento de datos cuenta con unidades redundantes de acondicionamiento térmico.
3. Ficha técnica del generador, cálculos de carga crítica respaldada, informes de pruebas de carga total o contratos de mantenimiento que permitan constatar que el generador puede abastecer todos los componentes críticos del centro de procesamiento de datos.

4. Planos eléctricos, listas de cargas conectadas, diagramas o actas de verificación técnica que evidencien que los sistemas de climatización están conectados a líneas respaldadas por el generador eléctrico.
5. Configuraciones del sistema de climatización, fichas de programación, capturas de consola de gestión o informes técnicos que permitan verificar la operación continua y los mecanismos automáticos de conmutación ante fallas.
6. Registros de pruebas, cronogramas de mantenimiento, listas de verificación o informes de resultados que evidencien que se testean periódicamente los mecanismos automáticos de failover en el sistema de climatización.
7. Actas de pruebas, bitácoras de mantenimiento, resultados de test de corte de energía o registros de alarmas que permitan verificar la operatividad del generador y de los sistemas UPS frente a condiciones reales.
8. Informes de revisión de diseño, análisis de impacto por crecimiento de carga o recomendaciones emitidas tras cambios tecnológicos que evidencien que se evalúa periódicamente la adecuación del diseño de redundancia.

Requisito CO.2 - Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia.

1. Diagramas de red, fotografías de la sala de comunicaciones, fichas técnicas de enlaces redundantes, actas de instalación o contratos con proveedores que permitan constatar que el centro de procesamiento de datos cuenta con infraestructura redundante a nivel de comunicaciones.
2. Facturas de servicios de conectividad, contratos activos con diferentes ISPs, informes de disponibilidad o configuraciones de balanceo de carga que evidencien la existencia de múltiples enlaces o proveedores de internet.
3. Capturas de consola de equipos de red, configuraciones de protocolos como VRRP, HSRP, entre otros, reportes de eventos o documentación de monitoreo que permitan verificar la detección automática de fallas en equipos críticos.

4. Diagramas de red actualizados, topologías con esquemas de redundancia, control de versiones de documentación o repositorios internos que permitan constatar que la arquitectura del centro de procesamiento de datos está correctamente documentada.
5. Cronogramas de pruebas, registros de resultados, tickets de verificación o bitácoras técnicas que evidencien la realización periódica de pruebas de failover de enlaces y equipos de red.
6. Informes técnicos de evaluación, actas de revisión de infraestructura, recomendaciones emitidas o matrices de puntos únicos de falla identificados que permitan verificar que se revisa el diseño de red con fines de mejora.
7. Informes de análisis de incidentes, registros de fallos, actas de reuniones técnicas, acciones correctivas implementadas o versiones modificadas de la arquitectura que evidencien que se evalúan eventos reales para ajustar la estrategia de redundancia y disponibilidad.

Requisito CO.4 - Planificar la continuidad de las operaciones y recuperación ante desastres.

1. Procedimientos operativos, planes de continuidad específicos, configuraciones de sistemas de alta disponibilidad o listas de acciones de contingencia que evidencien la existencia de medidas definidas para sistemas que soportan servicios críticos.
2. Listados de amenazas, mapas de riesgos, informes de análisis de continuidad o talleres de identificación de escenarios que permitan verificar que se ha realizado un relevamiento de amenazas que pueden afectar la operación.
3. Plan de backup, registros de ejecución de copias de seguridad, políticas de retención, reportes de verificación o capturas de consolas que evidencien la existencia de respaldos actualizados de sistemas críticos.

4. Planes de contingencia y recuperación vigentes, aprobaciones por parte de la alta dirección, control de versiones o publicación oficial interna que evidencien que están formalizados y validados los planes de contingencia y recuperación.
5. Matrices de criticidad o impacto, diagramas de dependencias, planillas de análisis de prioridades de recuperación, secciones del Plan de continuidad o Recuperación ante desastres (DRP/BCP) donde conste el orden definido para la recuperación, actas de aprobación del RSI o del CSI, o documentación utilizada para priorizar los servicios en simulacros o eventos reales.
6. Informe de Análisis de Impacto al Negocio (BIA) aprobado, matrices de procesos críticos, criterios de priorización o actas de validación que permitan constatar que se ha realizado un BIA con foco en continuidad.
7. Registros de pruebas específicas, cronogramas ejecutados, reportes de resultados o tickets internos que evidencien que se testean componentes parciales de los planes de forma controlada.
8. Acta de designación, estructura organizativa, roles y responsabilidades documentadas o referencias explícitas en los planes que permitan verificar quién es responsable de su mantenimiento y actualización.
9. Cronograma de pruebas, evidencias de simulacros integrales, informes de resultados o validaciones formales que permitan constatar que se prueba periódicamente la eficacia de los planes.
10. Actas de coordinación con proveedores, cláusulas contractuales sobre participación en pruebas, reportes de ejecución conjunta o registros de convocatorias que evidencien el involucramiento de terceros críticos según lo acordado.
11. Reportes de prueba, formularios de evaluación, tickets de seguimiento o bases de datos internas que permitan verificar que los resultados de las pruebas son documentados.
12. Registros de revisión posteriores a la prueba, planes de mejora, ajustes en los planes, lecciones aprendidas documentadas o versionado de documentos que demuestren que los resultados retroalimentan los planes y procedimientos.

Requisito CO.5 - Definir las ventanas de tiempo soportadas para la continuidad de las operaciones.

1. Acta de designación, roles definidos en el BIA, estructura organizativa, correos internos o referencias en procedimientos que evidencien quién o qué equipo está encargado de definir las métricas de recuperación para procesos críticos.
2. Tablas de BIA, anexos técnicos, fichas de procesos, criterios de continuidad documentados o reportes aprobados que permitan verificar que se ha establecido la máxima duración tolerable de interrupción (MTD) para cada sistema crítico.
3. Planillas técnicas, reportes del área de continuidad, matrices de recuperación o documentos de diseño que evidencien que se ha definido el tiempo objetivo de recuperación (RTO) de cada sistema.
4. Matrices de pérdida de datos tolerada, configuraciones de respaldo, informes de riesgos o procedimientos técnicos que permitan verificar que se ha definido el punto máximo de pérdida de datos aceptable (RPO) para cada sistema.
5. Análisis comparativos, informes de brechas, evaluaciones técnicas o planes de adecuación que evidencien que se comparan las métricas definidas con los niveles realmente alcanzables en la actualidad.
6. Registros de inclusión de RTO/RPO/MTD en planes de continuidad, criterios de validación utilizados en pruebas, actas de revisión técnica o plantillas de evaluación que demuestren que las métricas son insumo obligatorio en la planificación y ejecución de los planes de continuidad.
7. Actas de revisión, versiones de documentos técnicos, registros de cambios o tickets internos que evidencien que las métricas son revisadas cuando cambian procesos o tecnologías asociadas.
8. Informes de pruebas, gráficos de cumplimiento de objetivos, desviaciones detectadas y sus respectivas acciones correctivas que permitan verificar el contraste entre lo definido y lo logrado en los ejercicios de continuidad.

9. Informes de evaluación de inversiones, presentaciones a la dirección, matrices de priorización o comparativas técnicas-económicas que evidencien que se usan las métricas como insumo clave para tomar decisiones sobre infraestructura, automatización o redundancia.

Requisito CO.6 - Definir los mecanismos de comunicación e interlocutores válidos.

1. Política de comunicación, actas de designación, manual de gestión de crisis o correos institucionales que evidencien que las comunicaciones externas en situaciones críticas están restringidas a la Dirección o a su delegado.
2. Protocolos de autorización, registros de excepciones aprobadas, procedimientos que establecen restricciones o declaraciones de responsabilidad firmadas que permitan verificar que las áreas técnicas requieren aprobación explícita para comunicarse externamente.
3. Comunicaciones institucionales, publicaciones en intranet, manuales operativos o afiches internos que permitan constatar que se ha difundido quién es el vocero y por qué canales debe ser contactado.
4. Documento formal aprobado que contemple lineamientos estratégicos de comunicación ante crisis, incluyendo principios, objetivos, roles, audiencias, evaluación de eventos, nivel de comunicación, mensajes, medios, responsables y monitoreo, evidenciado mediante versiones controladas, anexos operativos o diagramas de flujo.
5. Registros de capacitación, listas de distribución, evidencias de lectura o actas de talleres que permitan verificar que todos los actores involucrados fueron informados sobre el contenido del plan y el procedimiento.
6. Cronogramas de ejercicios, reportes de simulacro, registros de participación o evidencia de ejecución coordinada con simulacros de continuidad o recuperación que permitan constatar que se prueba la respuesta comunicacional ante crisis.
7. Informes de auditoría, listas de chequeo, hallazgos documentados o planes de mejora derivados que evidencien que se evalúa formalmente el cumplimiento del plan y procedimiento de comunicaciones.

8. Informes posteriores al ejercicio, actas de revisión, acciones de mejora implementadas o versiones actualizadas de los documentos que permitan verificar que los resultados de revisiones y ensayos son utilizados para mejorar el plan.
9. Actas de aprobación, correos con observaciones de Dirección, minutas de revisión conjunta o registros de decisiones estratégicas que evidencien que la Dirección interviene en las actualizaciones del plan, especialmente en los mensajes y su forma de difusión.

5.13 Cumplimiento normativo y revisión

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito CN.1 - Cumplir con los requisitos normativos.

1. Matriz de cumplimiento normativo, listado de obligaciones legales, informes legales internos, actas del CSI sobre cumplimiento o registros de revisión que evidencien la identificación de requerimientos relacionados con seguridad, privacidad, acceso a la información y propiedad intelectual.
2. Actas de reunión, correos de coordinación, informes conjuntos o evidencias de actividades compartidas que permitan verificar la interacción entre el delegado de protección de datos personales y el RSI y/o CSI.
3. Procedimiento de actualización normativa, flujo de evaluación de cambios regulatorios, designación de responsables o registros de incorporación reciente que evidencien cómo se actualizan las obligaciones legales o normativas.
4. Correos institucionales, actas de comité, informes de cumplimiento o registros de entrega que evidencien que los resultados de las revisiones normativas o cambios legales son comunicados al RSI y/o al CSI para su análisis y seguimiento.

5. Informes de auditoría, cronogramas ejecutados, hallazgos documentados o registros de planes de acción que evidencien la realización de auditorías internas sobre cumplimiento normativo y legal.
6. Planes de mejora, registros de decisiones estratégicas, versiones actualizadas de políticas o procedimientos y actas del comité de seguridad que evidencien que los hallazgos de cumplimiento se utilizan como insumo para mejorar y tomar decisiones estratégicas.

Requisito CN.2 - Realizar auditorías independientes de seguridad de la información.

1. Informes de análisis de gap, matrices de madurez, listas de verificación de autoevaluación o actas del equipo de seguridad que evidencien que se ha realizado una evaluación comparando la situación actual frente a los requisitos del marco.
2. Listado de proyectos priorizados, presentaciones de planificación, cronogramas del plan de seguridad o actas del CSI que permitan verificar que las brechas detectadas alimentan el portafolio de iniciativas de seguridad.
3. Informes de auditoría interna, cronogramas ejecutados, actas de cierre o matrices de hallazgos que evidencien que se realiza anualmente una revisión formal interna del cumplimiento con el presente marco de seguridad.
4. Contratos con auditores externos, informes emitidos, planificaciones plurianuales o referencias en el programa de cumplimiento que evidencien la realización de auditorías externas del presente marco según una frecuencia establecida.
5. Planes de acción documentados, matrices de cumplimiento, tickets de implementación o reportes de seguimiento que permitan verificar que los hallazgos generan planes de acción y se realiza seguimiento hasta su cierre.
6. Informes de revisión de auditorías, encuestas de evaluación posteriores a su ejecución, análisis de cobertura o actas de mejora que evidencien que se

analiza la efectividad y suficiencia de las auditorías como insumo para futuras mejoras.

7. Términos de referencia, planes de auditoría, informes de resultados o listas de chequeo utilizadas que evidencien que las auditorías incluyen la totalidad del sistema de gestión de seguridad: objetivos, políticas y controles.

Requisito CN.3 - Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades.

1. Informes técnicos de revisión, contratos con terceros, actas de evaluación de sistemas o tickets internos que evidencien la realización de análisis puntuales sobre los sistemas de información.
2. Informes de pentest, cronogramas de pruebas, entregables de proveedores, actas de autorización o registros de ejecución que permitan verificar que se realizan pruebas de intrusión en sistemas críticos de forma periódica o tras cambios relevantes.
3. Correos de distribución de resultados, actas del CSI, registros de entrega de informes o minutas de reuniones que evidencien que los hallazgos de pruebas de seguridad son compartidos con los responsables correspondientes.
4. Procedimiento aprobado, manual de escaneo de vulnerabilidades, instructivos técnicos o flujos documentados que permitan verificar la existencia de un procedimiento formal con alcance a sistemas base y de aplicación.
5. Plan de escaneos, cronogramas ejecutados, logs de herramientas o entregables de pentest que evidencien que los escaneos se realizan cada 6 meses como máximo y las pruebas de intrusión anualmente en sistemas críticos.
6. Contratos o convenios con empresas especializadas, informes de terceros, certificaciones de ejecución o actas de coordinación que evidencien el involucramiento de especialistas externos en la revisión de vulnerabilidades y pruebas de intrusión.

7. Planes de acción derivados, ajustes documentados en configuraciones, versiones actualizadas de procedimientos o reportes de cierre que permitan constatar que los hallazgos se utilizan para fortalecer la seguridad de los sistemas.
8. Informes de revisión, listas de chequeo, hallazgos de auditoría interna o evidencias de monitoreo que demuestren que se verifica el cumplimiento del procedimiento de revisión periódica de vulnerabilidades.
9. Matriz de procesos de seguridad, cronogramas conjuntos o evidencias de coordinación operativa que permitan verificar que el procedimiento de revisión de vulnerabilidades forma parte activa de la gestión de seguridad de la información.

Requisito CN.4 - Gestionar las licencias de software.

1. Inventarios de licencias, registros de instalación en servidores, reportes de herramientas de gestión de activos o planillas de control que evidencien el seguimiento del estado de licenciamiento del software en equipos servidores.
2. Actas de designación, matrices de roles y responsabilidades, políticas internas o documentos operativos que identifiquen claramente quiénes gestionan la adquisición, asignación, renovación y baja de licencias.
3. Registros de licencias por equipo, informes de auditoría de los equipos entregados al personal, herramientas de inventario de software o planillas con correspondencia entre usuarios y licencias asignadas.
4. Planillas consolidadas, listados actualizados de software instalado por equipo, registros de licencias activas y su asignación o actas de revisión que permitan verificar que existe una trazabilidad razonable entre las licencias disponibles y las instalaciones detectadas.
5. Informes de utilización, comparativas entre licencias adquiridas y activas, reportes de auditoría o acciones de optimización que evidencien que se detectan posibles sobrelicenciamientos o subutilización.

6. Reportes legales o de cumplimiento, validaciones cruzadas con contratos de software, evaluaciones internas o actas de revisión que permitan constatar que se verifica el uso conforme a los términos de licenciamiento.

5.14 Protección de datos personales

Conjunto de posible evidencia que permite probar el cumplimiento de cada requisito incluido en esta sección.

Requisito PD.1 - Principio de legalidad

1. Planilla consolidada, registro interno, sistema de inventario o documento institucional que incluya el listado de bases de datos personales junto con su responsable, tipo de datos tratados y sistemas donde residen.
2. Comprobantes de registro emitidos por la URCDP, capturas del sistema de registro, certificados descargados o correspondencia oficial que evidencien que todas las bases de datos con datos personales están debidamente registradas.
3. Documentos internos de análisis legal, matriz de obligaciones por tipo de dato, referencias a la Ley N.º 18.331 y su reglamentación o informes del Delegado de protección de datos (DPD) que permitan verificar que se ha analizado qué normativa aplica a cada base de datos registrada.
4. Informes de verificación, actas de revisión por el DPD, listas de verificación de cumplimiento legal o registros de auditoría parcial que evidencien que se revisa regularmente la legalidad del tratamiento de datos personales.
5. Planes de acción documentados, tickets de corrección, evidencia de ajustes realizados en sistemas o procesos o reportes de cierre que permitan constatar que se actúa ante hallazgos de incumplimiento.
6. Programas de auditoría interna, informes con capítulos específicos sobre protección de datos, actas del CSI o cronogramas de evaluación que evidencien que se integra la revisión legal del tratamiento de datos personales como parte del proceso de auditoría.

Requisito PD.2 - Principio de veracidad
1. Formularios web, sistemas de gestión de solicitudes, canales habilitados (presencial, telefónico, correo institucional, etc.), instructivos internos o comunicaciones oficiales que evidencien que la organización ha definido mecanismos formales para que los titulares puedan solicitar la corrección manual de sus datos personales. 2. Formularios de trámites, procedimientos administrativos, instructivos internos o actas de revisión que permitan verificar que se define qué datos son necesarios y se limita su recolección sólo a los estrictamente requeridos por cada servicio o trámite. 3. Planillas de seguimiento, sistemas de atención al ciudadano, libros de registro, formularios archivados o reportes internos que evidencien que se documentan las solicitudes y los plazos de respuesta correspondientes. 4. Manual de atención, instructivos operativos, registros de atención presencial o capturas del sistema que permitan constatar que, cuando el titular está presente, se valida y actualiza la información en ese momento si corresponde. 5. Capturas de pantallas, reportes de funcionalidad en sistemas, cronogramas de revisión o registros de validación de datos que evidencien que se solicita periódicamente al usuario la revisión y corrección de sus datos personales. 6. Logs de auditoría, configuraciones de trazabilidad, capturas de sistemas, reportes de cambios o documentación técnica que permitan verificar que se registra quién modificó los datos, cuándo y qué cambió.

Requisito PD.3 - Principio de finalidad
1. Tickets de solicitud, capturas de sistemas, actas de eliminación manual, correos internos o registros de tareas que evidencien que se han eliminado datos personales que ya no eran necesarios para su finalidad original. 2. Formularios con cláusulas informativas, procedimientos internos, instructivos de registro o documentos de análisis de procesos que permitan verificar que se explicita la finalidad del tratamiento en cada instancia de recolección.

3. Tablas de retención, anexos a políticas de protección de datos, resoluciones internas o instructivos operativos que evidencien que existen criterios definidos para cuánto tiempo se conservarán los datos personales según su finalidad prevista.
4. Planillas de control, capturas de sistemas, logs de eliminación, actas de cumplimiento o formularios de seguimiento que evidencien que se registran las acciones de eliminación o anonimización siguiendo el procedimiento establecido.
5. Procedimientos aprobados, manuales técnicos, instrucciones operativas o registros de aplicación que permitan constatar que existen métodos definidos para eliminar o anonimizar datos una vez que su finalidad ha sido cumplida.
6. Cronogramas de revisión, listas de bases analizadas, registros de hallazgos o tickets de actualización que permitan verificar que se revisan periódicamente las bases para detectar datos cuya finalidad ya no se sostiene.
7. Planes de auditoría, informes de auditoría interna, listas de verificación o actas del CSI que evidencien que se revisa el cumplimiento de la finalidad como parte del proceso de auditoría institucional.

Requisito PD.4 - Principio de previo consentimiento informado

1. Capturas de formularios, textos legales en sitios web, registros de audio con aviso de consentimiento, formatos impresos o versiones de formularios que evidencien que se incluye la cláusula de consentimiento informado cuando corresponde.
2. Bases de datos con fecha y forma del consentimiento, logs del sistema, formularios firmados, correos electrónicos archivados o pantallazos de confirmación que evidencien que se guarda prueba del consentimiento cuando es requerido.
3. Listad de verificación legales, instructivos operativos, actas de análisis de bases de datos o comunicaciones con el DPD que evidencien que se evalúa si es necesario contar con consentimiento antes de iniciar el tratamiento de datos en cada caso.

4. Capturas de pantallas, pruebas de usabilidad, reportes de revisión legal o evidencias funcionales que demuestren que los formularios no preseleccionan la aceptación y permiten decidir de forma clara e informada.
5. Capturas del sitio web, instrucciones en formularios, correos con confirmación de baja o ejemplos de aplicación que evidencien que los titulares pueden retirar su consentimiento sin afectar el tratamiento previo.
6. Procedimiento vigente, instructivo del DPD, diagramas de flujo o matrices de decisión que establezcan cuándo se requiere consentimiento y cómo debe ser recabado, registrado y conservado.
7. Vínculos en el sitio web, materiales impresos, instructivos disponibles al público o comunicaciones institucionales que evidencien que los mecanismos para revocar el consentimiento están visibles y accesibles.
8. Planes de auditoría, informes con revisión específica del consentimiento, listas de verificación o hallazgos documentados que evidencien que este aspecto es revisado regularmente.
9. Versiones actualizadas de formularios, actas de revisión legal, tickets de mejora o evidencias de ajustes implementados que permitan constatar que los medios y textos utilizados para recabar consentimiento se actualizan periódicamente.

Requisito PD.5 - Principio de seguridad de los datos

1. Listados de permisos, configuraciones de control de acceso, evidencias de autenticación nominada o reportes de revisión de perfiles que permitan verificar que solo acceden quienes lo requieren, con el mínimo nivel necesario.
2. Registros de acceso a oficinas, sistemas de cerraduras controladas, cajas fuertes, controles de archivadores o actas de control que evidencien que se protege el acceso físico a información personal en papel.
3. Políticas de seguridad, controles implementados, procedimientos operativos y registros de concientización que evidencien la implementación de salvaguardas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

4. Planillas, tickets, reportes de incidentes o logs de herramientas de gestión que permitan verificar que se registran eventos con detalle de fecha, tipo de incidente y si involucró datos personales.
5. Logs de acceso, configuraciones de sistemas de trazabilidad, capturas de herramientas o reportes exportables que evidencien que se puede identificar quién accedió, cuándo y a qué tipo de información sensible.
6. Procedimiento formal vigente, flujos de escalamiento, modelos de formulario o registros de notificación a la URCDP que permitan constatar que se cumple con el plazo y contenido exigido por la normativa.
7. Documentación aprobada, plantillas de comunicación, cronogramas de aviso o actas de activación de protocolo que evidencien que está definido cómo se informa a los titulares cuando sus datos personales se ven comprometidos.
8. Informes de simulacro, reportes de escenarios probados, registros de participación o hallazgos documentados que evidencien que se prueba la eficacia de las medidas ante eventos como accesos indebidos o fugas de información.
9. Actas de revisión de riesgos, presentaciones ejecutivas, planes estratégicos de seguridad o decisiones de alto nivel que permitan verificar que la dirección evalúa y toma decisiones sobre la protección de datos personales.

Requisito PD.6 - Principio de reserva

1. Listas de control de acceso, matrices de permisos, evidencias de segregación de funciones o registros de revisión de accesos que permitan constatar que solo accede el personal cuya función lo justifica según la finalidad del tratamiento.
2. Políticas de acceso, matrices de roles y finalidades, manuales operativos o anexos de procedimientos que identifiquen claramente qué roles pueden acceder a qué datos y con qué propósito.
3. Cláusulas en contratos laborales, reglamentos internos, códigos de conducta o políticas institucionales aprobadas que evidencien la existencia de sanciones en caso de uso indebido o divulgación de datos personales.

4. Contratos laborales con cláusula de confidencialidad, acuerdos específicos firmados, reglamentos internos aceptados o registros de firma digital que permitan verificar que el personal autorizado se compromete formalmente a guardar confidencialidad.
5. Listados normativos, códigos de ética, políticas internas o anexos específicos que definan con claridad qué acciones se consideran una violación al principio de reserva en el tratamiento de datos personales.
6. Documento de procedimiento aprobado, flujos de tratamiento de incidentes disciplinarios, modelos de informe o registros de aplicación que evidencien que existe un procedimiento estructurado para investigar este tipo de situaciones.
7. Formularios internos, tickets de solicitud, correos institucionales con aprobación o registros de control que permitan verificar que toda solicitud de acceso a datos personales incluye su finalidad y ha sido autorizada por el responsable correspondiente.

Requisito PD.7 - Principio de responsabilidad proactiva

1. Políticas institucionales, instructivos de desarrollo o mejora de procesos, formularios de análisis de privacidad o actas de revisión de proyectos que evidencien que se contemplan criterios de privacidad desde el diseño y configuración inicial.
2. Actas de participación del DPD, correos de consulta, observaciones en documentos de diseño o evidencia de asesoramiento documentado que permitan verificar su intervención en medidas técnicas u organizativas relacionadas con privacidad.
3. Informes de análisis posterior al incidente, tickets de modificación, actas de evaluación de impacto o registros de revisión técnica que evidencien que se revisa la efectividad de las medidas de privacidad ante cambios en procesos o incidentes.
4. Cronogramas de revisión, informes técnicos, actas del CSI o matrices de evaluación que permitan constatar que se analiza regularmente la efectividad de las medidas implementadas.

5. Tickets de mejora, nuevas versiones de configuraciones, actualizaciones de controles o decisiones registradas que evidencien que las revisiones periódicas resultan en ajustes concretos a las medidas técnicas aplicadas.

Requisito PD.8 - Derechos de los titulares de los datos

1. Registros de entrada de solicitudes, tickets de atención, correos institucionales o planillas internas que evidencien que la organización recibe y da curso a los pedidos de los titulares de datos personales.
2. Planillas con fechas de recepción y respuesta, reportes de cumplimiento de plazos, indicadores operativos, emails recibidos y su respuesta o otros registros de respuesta dentro de los días hábiles establecidos por la legislación que permitan verificar el cumplimiento de dicho plazo legal.
3. Actas de asignación, roles definidos en el procedimiento, estructura organizativa o correos internos que permitan verificar quiénes son responsables de cada etapa del proceso.
4. Planillas de seguimiento, registros en sistemas internos, actas de tratamiento o archivos documentales que evidencien el control del ciclo completo de cada solicitud (recepción, evaluación, respuesta).
5. Procedimiento o instructivo que incluya los derechos de información, acceso, actualización, rectificación, inclusión, supresión e impugnación, con flujos o formatos diferenciados por tipo de derecho.
6. Procedimiento documentado, formulario con validación, requerimientos de documentación, instrucciones operativas o plantillas que evidencien cómo se verifica la identidad del titular antes de responder a una solicitud.
7. Publicación en sitio web, cartelería institucional, materiales entregados al personal o correos informativos que permitan constatar que los procedimientos para ejercer los derechos son conocidos por todas las partes relevantes.
8. Tableros o dashboards, informes mensuales, métricas de cumplimiento o reportes del DPD que evidencien que se generan indicadores de desempeño sobre el procedimiento de gestión de solicitudes de derechos de los titulares

(como volumen de solicitudes, tiempo medio de respuesta o proporción de rechazos, entre otros).

9. Actas de revisión, cronogramas ejecutados, tickets de mejora o reportes de hallazgos que permitan verificar que el procedimiento se revisa regularmente y se documentan desvíos u oportunidades de mejora.
10. Versiones actualizadas del procedimiento, cambios registrados en instructivos, plan de acción implementado o tickets cerrados que evidencien que las mejoras detectadas se incorporan de forma efectiva.