SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

TOMÉ, 28 OCTUBRE 2025

VISTOS:

Considerando el Decreto Fuerza Ley N° 01/24.04.2006 del MINSAL; el D.F.L. N° 29/2004 sobre Estatuto Administrativo; la Ley N° 19.880 sobre Bases de los Procedimientos Administrativos; la Resolución N° 6/2019 de Contraloría sobre exención de toma de razón en materias de personal; los Decretos Supremos de Salud N° 140/2005 y N° 38/2005 que aprueban los Reglamentos Orgánicos de los Servicios de Salud y de los Establecimientos de Salud de Menor Complejidad; la Resolución Exenta N° 2778/2023 del SSThno; la Resolución Exenta N° 1251/2023 que aprueba la Política General de Seguridad de la Información del Hospital de Tomé; el COMGES 2025; y el Ordinario N° 943/2025 del Subsecretario de Redes Asistenciales sobre implementación de controles críticos de seguridad de la información según ISO/IEC 27001:2022; que, conforme al D.S. N° 285/2022 y la Ley N° 21.663 de Ciberseguridad, el Hospital de Tomé se encuentra incluido en la lista preliminar de **Operadores de Importancia Vital (OIV)**; y que, mediante la Providencia N° DHT-6553 y el oficio N° 0106 clasificado como secreto, se instruye evacuar un Informe Técnico Fundado respecto del cumplimiento de los criterios del artículo 4° del D.S. N° 285/2022, se da curso a la presente comunicación.

CONSIDERANDO:

1. Que la gestión adecuada de los incidentes de seguridad de la información es fundamental para proteger la confidencialidad, integridad y disponibilidad de los activos de información del Hospital de Tomé.
2. Que el Hospital de Tomé requiere establecer procedimientos claros para la identificación, registro, análisis, gestión y resolución de incidentes de seguridad de la información, asegurando respuestas oportunas y efectivas ante cualquier eventualidad.
3. Que la correcta implementación de este procedimiento garantiza el cumplimiento de las normativas nacionales, estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27002:2022, y demás requerimientos legales, incluyendo la Ley N° 19.628, Ley N° 20.285, Ley N° 21.180, Ley N° 21.459 y Ley N° 21.663.
4. Que este procedimiento aplica a todos los funcionarios, personal a honorarios, proveedores y terceros que interactúen con los sistemas de información del Hospital de Tomé, asegurando la correcta gestión de incidentes y la protección de los activos de información.
5. Que la implementación de este procedimiento contribuye a formalizar roles y responsabilidades, mecanismos de comunicación, escalamiento de incidentes, planes de mitigación, auditorías y medidas correctivas en el marco de la seguridad de la información.

RESUELVE EXENTA N° 2122

1. **APRÚEBASE** el Procedimiento de Gestión de Incidentes de Seguridad de la Información del Hospital de Tomé, que establece lineamientos, responsabilidades, flujos de trabajo y mecanismos de control para la identificación, registro, análisis, gestión, mitigación, resolución y cierre de incidentes de seguridad de la información,

en concordancia con normas nacionales, estándares internacionales y buenas prácticas de ciberseguridad.

2. **DISPÓNGASE** que todos los funcionarios, colaboradores, personal a honorarios y proveedores externos que operen en el Hospital de Tomé cumplan estrictamente con los lineamientos establecidos en este procedimiento, incluyendo:
   a) Notificación inmediata de incidentes de seguridad de la información.
   b) Registro completo y preciso de los incidentes en las herramientas habilitadas.
   c) Clasificación y análisis de la criticidad de cada incidente.
   d) Aplicación de medidas de mitigación y contingencia según protocolos internos.
   e) Escalamiento oportuno a las autoridades competentes según la gravedad del incidente.
   f) Monitoreo, auditoría y cierre documentado de cada incidente.
   g) Cumplimiento con la Política General de Seguridad de la Información.
   h) Protección de datos personales, confidencialidad y propiedad intelectual.
   i) Uso adecuado de recursos, sistemas y equipos del Hospital de Tomé.
3. **ENCÁRQUESE** a la Jefatura de Tecnología de la Información, al Encargado de Seguridad de la Información y a las áreas responsables de los sistemas y servicios críticos la supervisión, aplicación, monitoreo y control del cumplimiento de este procedimiento, así como la gestión de incidentes, auditorías y medidas correctivas en caso de incumplimiento.
4. **DEJASE CONSTANCIA** que todo funcionario, colaborador o proveedor que interactúe con los sistemas de información del Hospital de Tomé deberá aplicar y comprender este procedimiento y cumplir con todos los lineamientos, directrices y procedimientos establecidos, reportando incidentes y asegurando la correcta gestión de los activos de información.
5. **ESTABLÉCESE** que la presente resolución entra en vigor a partir de su publicación, y cualquier modificación futura deberá efectuarse mediante resolución exenta de la autoridad competente, asegurando la coherencia con las normativas legales y estándares internacionales aplicables.

"ANÓTESE Y COMUNÍQUESE"

LEC/CCU/ccu
N° INT. 04/28.10.2025
DISTRIBUCIÓN:

- Subdirección Administrativa H. Tomé
- Subdirección Médica H. Tomé
- Oficina de Partes Hospital de Tomé
- CR. Apoyo Diagnóstico
- Área Recursos Físicos
- Área Gestión y Desarrollo de las Personas
- CR. Atención Cerrada
- CR. Atención Abierta
- CR. Emergencia

FIRMA DIRECTOR HOSPITAL DE TOMÉ

Firmado por Aníbal Antonio Cea Henríquez
Fecha 28/10/2025 15:09:16 CLST

PROC03-25-0002

PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad de la Información – Hospital de Tomé

Versión Oficial Actual 1 – Julio 2025

CONTENIDO

1 PROPÓSITO.

Establecer las actividades necesarias en el Hospital de Tomé, para la detección oportuna y tratamiento de vulnerabilidades o eventos que comprometan la seguridad de los Activos de Información de la Institución.

Establecer responsabilidades de las distintas Unidades con relación a la seguridad de los datos institucionales (integridad, disponibilidad y confidencialidad), ya sea se encuentren en la plataforma informática como en su manipulación a cargo de los funcionarios en general.

Responder en forma rápida, eficaz y ordenada ante la ocurrencia de incidentes de seguridad que afecten los activos de información institucionales.

Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

2 ALCANCE.

Este procedimiento aborda la gestión de incidentes de seguridad que afecten a los activos de información del tipo: base de datos, documento, equipo, expediente, formulario, infraestructura física, persona, sistema de información, software, en cuanto a la:

- Confidencialidad: acceso no autorizado a la información.
- Integridad: Modificación no autorizada, destrucción o pérdida de información.
- Disponibilidad: Inaccesibilidad a la información.

Este procedimiento es aplicable a todos los funcionarios[1] (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Hospital de Tomé y que tengan derechos de acceso a la información que puedan afectar los activos de información del Establecimiento.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información		
Estándar	**ID Control**	**Nombre del Control**
ISO 27001:2022	A 05.5	Contacto con las autoridades
	A 05.6	Contacto con grupos de interés especial
	A 06.8	Notificación de los eventos de seguridad de la información
	A 06.8	Notificación de puntos débiles de la seguridad

[1] A lo largo del procedimiento cada vez que se mencione funcionario se refiere a: funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.).

Alcance de Dominios y Controles de Seguridad de la Información		
	A 05.09	Inventario de información y otros activos asociados
	A 05.13	Etiquetado de la información
	A 05.24	Responsabilidades y procedimientos
	A 05.26	Respuesta a incidentes de seguridad de la información
	A 05.27	Aprendizaje de los incidentes de seguridad de la información
	A 05.28	Recopilación de evidencias

3 TERMINOLOGÍA.

- **Amenaza:** Potencial causa de un incidente que podría dañar la organización o sus activos de información. Las amenazas pueden ser internas o externas, intencionales o accidentales.
- **Ciberataque**: Actividad intencional realizada por actores internos o externos que busca explotar vulnerabilidades para acceder, modificar, interrumpir o destruir información, sistemas o servicios.
- **Clasificación de Incidentes:** Proceso de evaluación del incidente para determinar su severidad y priorización, utilizando criterios como impacto operativo, alcance, activos afectados y probabilidad de recurrencia.
- **CSIRT:** Grupo designado responsable de coordinar y ejecutar las actividades de respuesta a incidentes, compuesto por especialistas en seguridad, TI y, según corresponda, representantes.
- **Evento de Seguridad**: Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad.
- **Gestión de Incidentes:** Proceso estructurado para identificar, analizar, responder y aprender de los incidentes de seguridad con el objetivo de minimizar daños y prevenir su recurrencia.
- **Incidente de Seguridad:** Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones institucionales y amenazar la seguridad de la información.
- **Lecciones Aprendidas:** Análisis posterior a un incidente que identifica oportunidades técnicas o administrativas de mejora en los procesos, controles y respuesta para prevenir futuros incidentes o mejorar la gestión.
- **Notificación de Incidentes:** Proceso formal de comunicar a las partes interesadas internas y externas sobre la ocurrencia de un incidente, su impacto y las medidas de mitigación implementadas, conforme a los requisitos legales y contractuales.

- **Recuperación:** Etapa del proceso de gestión de incidentes enfocada en restaurar las operaciones normales de los sistemas y servicios afectados, garantizando la seguridad y estabilidad.
- **Registro de Incidentes:** Documento o sistema utilizado para registrar, rastrear y gestionar incidentes de seguridad, incluyendo detalles como la naturaleza del incidente, su clasificación, impacto y acciones tomadas.
- **Resiliencia Cibernética:** Capacidad de los sistemas y servicios de la organización para resistir, recuperarse y adaptarse frente a incidentes de seguridad, minimizando el impacto en las operaciones.
- **Respuesta a Incidentes:** Conjunto de acciones específicas ejecutadas para contener, mitigar, investigar y resolver un incidente de seguridad, asegurando la continuidad de negocio.
- **Riesgo de Seguridad:** Combinación de la probabilidad de que ocurra un incidente y las consecuencias negativas asociadas.
- **Vulnerabilidad:** Debilidad en un sistema, proceso o configuración que puede ser explotada para comprometer la seguridad de la información o los sistemas.
- **ANCI:** Agencia Nacional de Ciberseguridad.
- **TI:** Tecnologías de la Información

4 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS.

- **Marco Normativo.**
  - NCh ISO27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información.
  - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
    - Decretos Supremos y Normas Internacionales de Seguridad de laInformación y Ciberseguridad.
    - **Normas relacionadas:**
      - Ley N° 18.845, de 1989, que establece sistema de microcopia o micro grabación de documentos.
      - Ley N° 19.799, sobre documentos y firmas electrónicas
      - Ley N° 19.880 de bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado.
      - Ley N° 20.217, que modifica el Código de Procedimiento Civil y la ley N° 19.799, sobre documento electrónico, firma electrónica y los servicios de certificación de dichas firmas.
      - Ley N° 20.584, de derechos y deberes de los pacientes frente a las acciones y prestaciones de salud.

- Ley N° 21.180 Ley de Transformación Digital del Estado, establece directrices para la modernización de los procesos y servicios digitales en instituciones públicas. Tiene implicaciones en la privacidad y la protección de datos personales, ya que establece estándares para la seguridad de la información en servicios y plataformas digitales, fomentando la eficiencia sin comprometer la confidencialidad y la integridad de los datos de los ciudadanos.
- Ley N° 21.663 sobre Marco de Ciberseguridad, esta ley proporciona un marco para asegurar la ciberseguridad de infraestructuras críticas, que indirectamente impacta en la protección de datos.
- Decreto N° 295, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba reglamento de reporte de incidentes de ciberseguridad de la ley N° 21.633.
- Ley 21.668 establece la interoperabilidad de las fichas clínicas, sobre protección de datos establece un marco legal para salvaguardar la privacidad y los derechos de los ciudadanos en relación con sus datos personales.
- Decreto N° 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción, Subsecretaría de economía, que aprueba el Reglamento de la ley N° 19799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
- Decreto N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo, Subsecretaría de Economía y empresas de menor tamaño, que modifica el decreto N° 181, de 2002, que aprueba Reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma y deroga los decretos que indica.
- DFL N° 1, de 15 de marzo de 2021, del Ministerio de las Culturas, las artes y el patrimonio, que determina los requisitos del método de elaboración, conservación y uso de las microformas y de aquellos a emplear en la destrucción de documentos originales en virtud de la ley N° 18.845.
- Decreto N° 23, de 21 de octubre de 2021, que aprueba el reglamento que establece los medios y procedimientos técnicos y administrativos que se utilizarán en la generación de microformas.
- DFL N° 1, 2005, Ministerio de Salud.
- Decreto N° 41, de 2012, del Ministerio de Salud, Reglamento de ficha clínica.
- DFL N° 725, de 31 de enero de 1968, Código Sanitario.
- Decreto 273, de 2022, que establece la obligación de reportar incidentes de ciberseguridad a los organismos del Estado al CSIRT de gobierno.
- El Decreto N° 533 establece el marco regulatorio en ciberseguridad para las instituciones públicas en Chile, que incluye normas para la protección de la información, la gestión de incidentes de ciberseguridad y la protección de infraestructuras críticas, en las que se procesan datos personales.
- El Decreto Supremo N° 7 establece una Norma Técnica de Seguridad de la Información y Ciberseguridad, en concordancia con la Ley Nº 21.180 sobre

Transformación Digital del Estado. Que tiene el objetivo de definir estándares mínimos de seguridad y ciberseguridad para todos los órganos de la administración pública en Chile, contribuyendo a la protección de los datos personales y a la seguridad de la información en los sistemas digitales gubernamentales.

5 ROLES Y RESPONSABILIDADES.

- **Funcionarios.**
  - Manejar, utilizar y proteger el acceso a los documentos institucionales, asegurando su integridad, disponibilidad y confidencialidad en los procesos y sistemas institucionales.
  - Informar de manera oportuna cualquier evento, debilidad o sospecha de incidente de seguridad que pueda comprometer la información institucional, a través de los canales oficiales establecidos por el Hospital de Tomé.

- **Encargado de Seguridad de la información y Ciberseguridad.**
  - Diseñar, actualizar y garantizar el cumplimiento del procedimiento de gestión de incidentes.
  - Supervisar la implementación de acciones correctivas y preventivas.
  - Actuar como enlace principal entre la alta dirección, partes interesadas internas y externas, y otras áreas relevantes.
  - Informar a la alta dirección sobre incidentes críticos y coordinar respuestas estratégicas.
  - Gestionar y priorizar eventos e incidentes, liderando la ejecución de medidas para mitigar riesgos y prevenir recurrencias.
  - Encargado de Informar a CSIRT de Gobierno, Incidentes de Seguridad de acuerdo con lo indicado en Decreto 273, de 2022 y Ley N° 21.180.

- **Área de Tecnologías de la Información y Comunicación.**
  - Proporcionar soporte técnico en la gestión de incidentes que afecten los sistemas y la infraestructura tecnológica de su administración.
  - Identificar y remediar vulnerabilidades explotadas en incidentes.
  - Proporcionar logs, configuraciones y otros datos técnicos para el análisis de los incidentes.
  - Coordinar a las unidades internas de Operaciones TI y Tecnologías Digitales.
  - Implementar medidas de recuperación y restauración de servicios afectados.

- **Unidades responsables de procesos.**
  - Dar cumplimiento a las políticas de seguridad de la información, aplicar el presente procedimiento y gestionar los incidentes en lo que se refiere al uso, manipulación y

protección de acceso a datos institucionales de modo de garantizar su integridad, disponibilidad y confidencialidad.
- Representar los intereses de las áreas afectadas y colaborar en la gestión del impacto de los incidentes en los procesos de unidades responsables.
- Informar sobre incidentes detectados en sus áreas.
- Apoyar en la evaluación del impacto del incidente en sus procesos.
- Implementar las recomendaciones para mitigar riesgos futuros en su ámbito.

- **Equipo de Respuesta de Incidentes.**
  - Supervisar que los Equipos o Áreas Resolutoras gestionen los incidentes de manera adecuada y conforme a su nivel de criticidad.
  - Gestionar los incidentes de acuerdo con el nivel de criticidad.
  - Coordinar la respuesta a incidentes de alto impacto con apoyo de las siguientes áreas:
    - ✓ Recursos Físicos.
    - ✓ Recursos Humanos.
    - ✓ Gestión del Cuidado
    - ✓ Unidad Jurídica.
    - ✓ Finanzas
    - ✓ Unidades responsables de los datos afectados.

- **Equipos o Áreas resolutoras designadas para la gestión de incidentes.**

  - Será responsable de:
    - ✓ Coordinar la activación de los equipos de respuesta ante incidentes.
    - ✓ Identificar la causa raíz de los incidentes y proponer medidas correctivas.
    - ✓ Generar y mantener reportes documentados sobre la gestión de incidentes.
    - ✓ Realizar el seguimiento de las medidas de mitigación hasta su cierre.
    - ✓ Mantener comunicación activa con CSIRT de Gobierno u organismos relevantes para la gestión de incidentes.

Nota: El personal designado deberá contar con un respaldo que lo reemplace en caso de ausencia.

Todos los usuarios, Administradores de Seguridad, Custodio de las Datos, las Unidades de Informática, Jefes de Servicio, Directivos, Jefes de Área, Jefes de Unidades y Gestión de Personas son responsables del cumplimiento de este procedimiento.

6 PROCEDIMIENTO.

6.1 Notificación de un incidente de seguridad.

Todo el personal, incluidos funcionarios, personal a honorarios y terceros, debe informar de manera inmediata cualquier debilidad, evento, incidente, amenaza o riesgo que pueda comprometer la seguridad de los activos de la organización. Para ello, el Hospital de Tomé dispone de los siguientes canales de comunicación únicos:

- **Contacto Telefónico:**
  - 415016
- **Mesa de Servicio TI:**
  - Temas de seguridad (eventos, debilidades de seguridad, incidentes, amenazas, riesgos): https://tic.hospitaldetome.cl
    - Categoría: Seguridad, subcategoría Incidente de Seguridad*

Es obligatorio utilizar estos canales oficiales para garantizar una gestión oportuna, segura y eficiente de los incidentes reportados.

***Nota**: Para asegurar una correcta reserva en los datos de seguridad se solicita que al momento de reportar la incidencia se indique correctamente la **categoría** la cual debe ser Seguridad, Incidente de Seguridad.

6.2 Gestión de Incidentes.

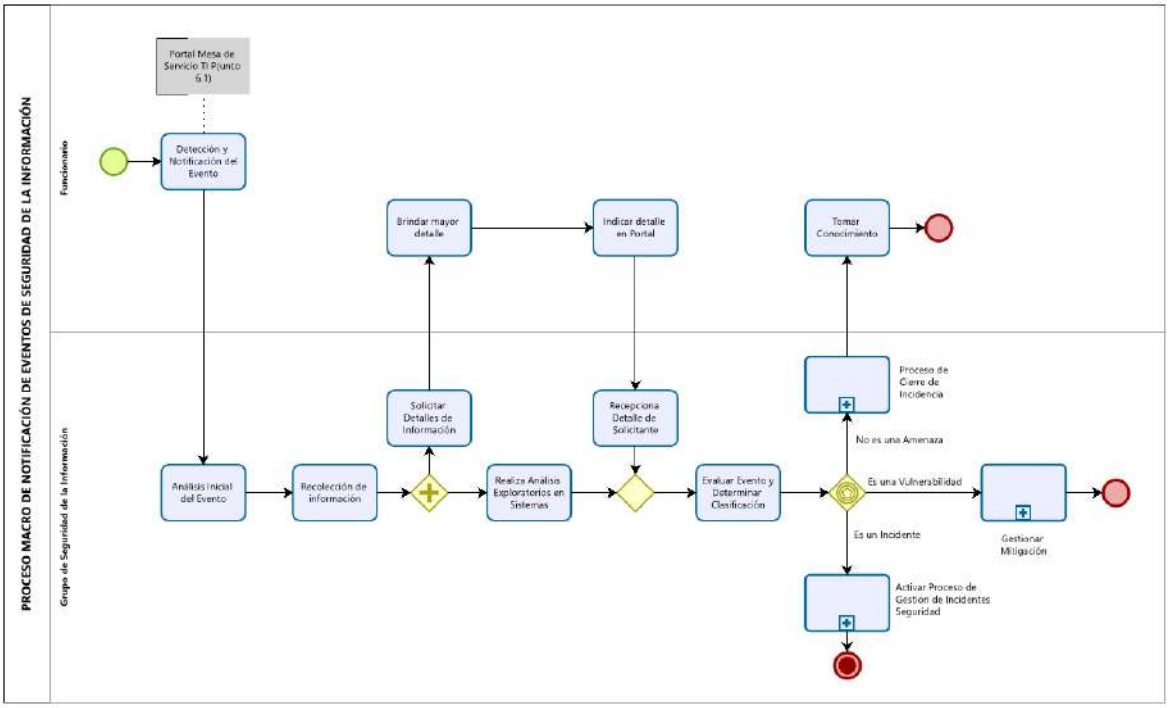
La institución llevará adelante la respuesta a incidentes a través de sus instancias técnicas y se coordinará con el equipo de respuesta a Incidentes y/o el Comité de Seguridad, en la medida que el impacto de los incidentes afecte a los activos vitales de la organización.

Los problemas relacionados a los incidentes de seguridad de la información dentro de la organización serán manejados por el Encargado de Seguridad de la Información y Ciberseguridad, el que se apoyará en el personal equipo de respuesta a Incidentes y/o el Comité de Seguridad, con atención al resguardo de los principios de la Política General y las leyes vigentes. A su vez, el Encargado de Seguridad de la información y Ciberseguridad mantendrá los contactos correspondientes con las autoridades, grupos de interés externos o foros que manejen los problemas relacionados con los incidentes de seguridad de la información.

Cabe destacar que en la medida que los incidentes hayan sido judicializados, se requerirán de especiales cuidados, en orden a convocar a los expertos policiales para que accedan a la información necesaria para la investigación.

6.3 Reporte de eventos y debilidades en la Seguridad de la Información.

6.3.1 Flujo de la notificación.



Todo el personal del Hospital de Tomé, en coordinación con su jefatura, es responsable de notificar cualquier tipo de evento que pueda afectar el funcionamiento normal del Sistema de Seguridad de la Información de la Institución.

Cada evento o incidente de relevancia se consignará en el sistema de tickets dispuesto por el Hospital de Tomé (Punto 6.1) como herramienta central de registro y gestión de los incidentes, con objetivo central de concentrador y notificador de éstos, y, en consecuencia, disponer de un registro central de los incidentes.

En la herramienta centralizada de reporte y notificación de incidentes quedarán registradas también las actividades de administración de incidentes para poder evaluar los procesos involucrados (mejora continua) incorporando a ella aprendizajes obtenidos ante errores y/o aciertos de los planes de acción ejecutados.

Esta función es importante para la institución, pues en la medida que los funcionarios están alertas a estos detalles se maximiza la vigilancia y resguardo de los activos institucionales.

En este sentido todos los funcionarios deberán siempre estar alertas tanto a los temas de respeto a las políticas de seguridad de la información como a señales que parezcan extrañas o poco habituales, teniendo en consideración que cada uno de ellos puede ser blanco u objetivo de un ataque cibernético mediante el cual se puede acceder a información personal o institucional relevante, entre la que destaca en primera instancia:

Credenciales o contraseñas.

- Direcciones de correo electrónico.
- Perfiles de usuario o gustos personales de compras y/o navegación web.
- Información confidencial (documentos sensibles institucionales, tarjetas de crédito, entre otros).
- Recursos del sistema (CPU, USB y disco externos), para almacenar malware o utilizar equipos institucionales sin autorización.

Según el impacto del evento, el Encargado de Seguridad de la Información debe contactar a la persona que reporta y Jefatura del área relevante en un plazo no superior a 24 h, para recolectar toda la información necesaria para el análisis del evento, registrando todos los antecedentes.

Hecha la recolección de información sobre el incidente, el Encargado de Seguridad de la Información y Ciberseguridad debe analizar los antecedentes. El resultado de dicho análisis puede tener las siguientes opciones:

a) **El evento no corresponde a una amenaza**: se cierra el registro de eventos, informando a la persona que reportó.

b) **El evento corresponde a una vulnerabilidad**: se gestiona las actividades de mitigación (con los dueños de los activos comprometidos, el área o unidad de competencia y/o Comité de Seguridad), dejando registro de la gestión de la vulnerabilidad.

c) **El evento ocurrió y debe ser gestionado como incidente**: se activa el proceso de Gestión de Incidentes de Seguridad.

Identificar Equipos/Áreas Resolutoras por tipo de Incidentes.

Se deben asociar Equipos particulares o Áreas generales, como resolutores para abordar incidentes según su naturaleza, lo que debe quedar documentado para servir de guía de asignación de los incidentes una vez declarados.

6.3.2 Reporte de Incidentes de Ciberseguridad a la ANCI: Procedimiento y Plazos

Tras la detección inicial de un incidente de ciberseguridad, es **obligatorio** para las instituciones del Sector Salud generar un reporte formal y detallado. Este documento es crucial para la documentación exhaustiva del incidente y para la comunicación oficial con las autoridades competentes, en particular con la Agencia Nacional de Ciberseguridad (ANCI). Es por esta razón que cuando se determine que un Evento de Seguridad notificado por la Mesa de Servicio es efectivamente un incidente de seguridad se deberá crear un Incidente de tipo "Grave" y asociar el evento inicial del Solicitante.

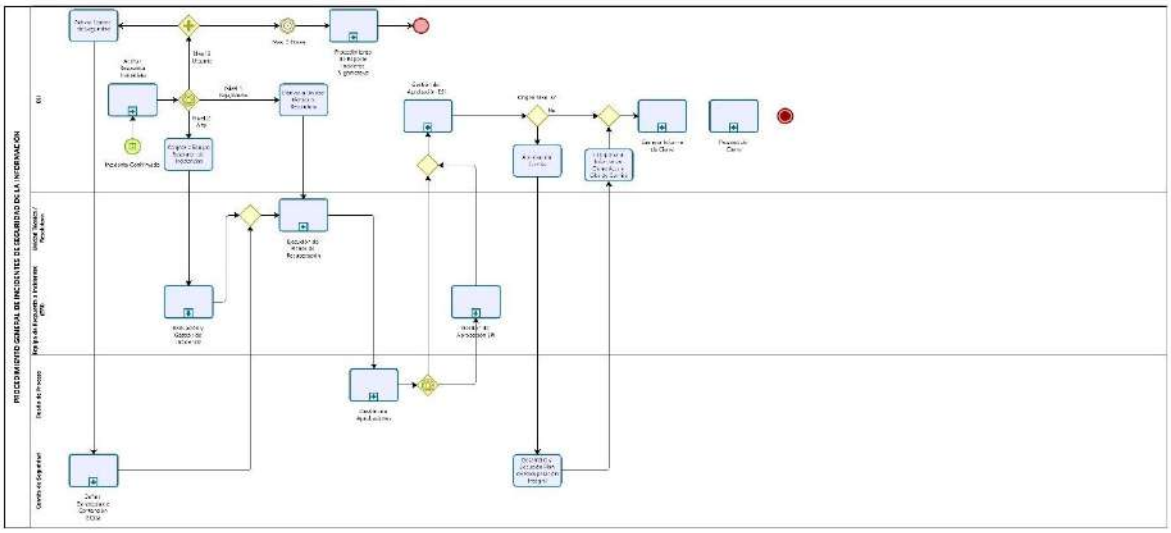
Obligatoriedad del Reporte: De acuerdo con el Artículo 3° del Decreto N° 295/2024, que aprueba el reglamento de reporte de incidentes de ciberseguridad, todos los organismos del Sector Salud que presten servicios esenciales están obligados a reportar aquellos incidentes que se consideren de impacto significativo, según los criterios definidos en dicho decreto.

Plataforma Oficial de Reporte (ANCI): Para facilitar y estandarizar el proceso de reporte de incidentes, la ANCI ha dispuesto la plataforma oficial **portal.anci.gob.cl**. Las instituciones del Sector Salud deberán utilizar este sitio web para notificar sus incidentes significativos.

6.4 Procedimiento para gestión de Incidentes.

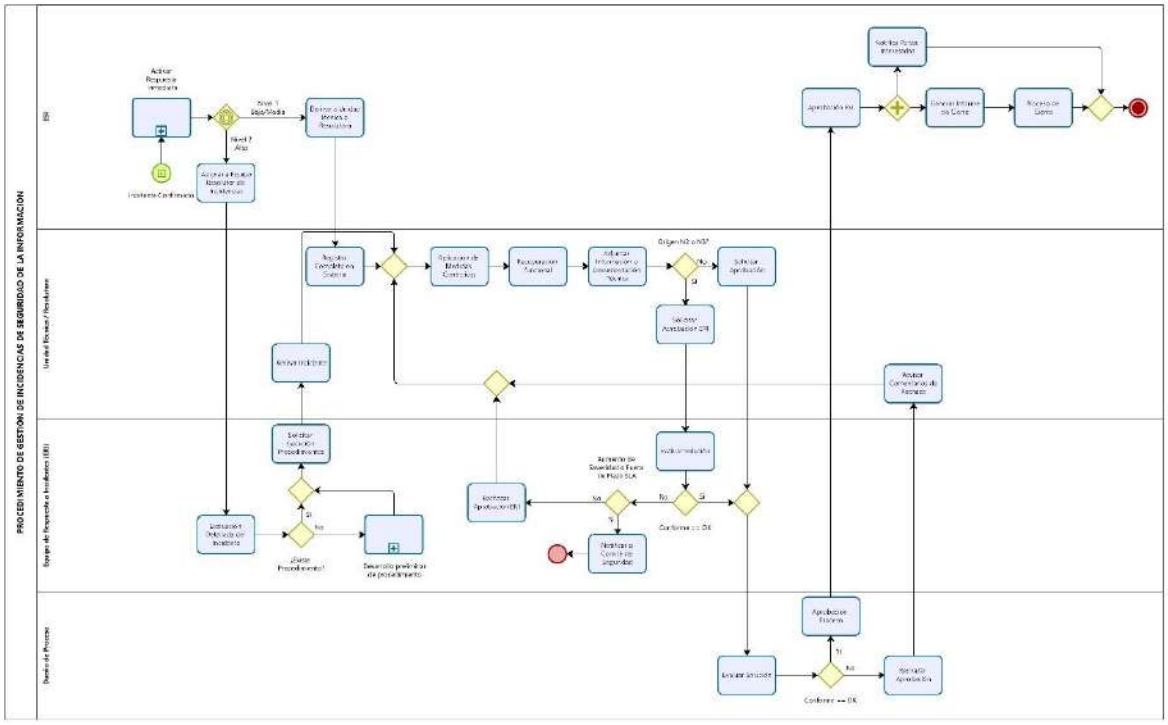
A continuación, se presentan los procedimientos que debe ejecutar las Áreas Técnicas para cumplir con el resguardo de la plataforma y datos que le competen, de acuerdo con niveles de resolución dependiendo de la clasificación del Incidente de Seguridad.

6.4.1 Flujo General del proceso.



El proceso de Gestión de Incidentes de Seguridad de la Información inicia cuando se confirma la existencia de un incidente. A partir de ahí, el Encargado de Seguridad de la Información (ESI) clasifica el incidente según su prioridad, lo que define su nivel de gestión (Nivel 1, 2 o 3). Para todos los niveles se activa la respuesta inmediata, que contempla acciones de contención, recolección de evidencia y notificaciones básicas. Si el incidente es clasificado como Nivel 1, se gestiona directamente mediante el equipo resolutor correspondiente, avanzando hacia la recuperación, análisis de causas y cierre del caso. En el caso de Nivel 2, el ESI puede activar al Equipo de Respuesta a Incidentes (ERI). Si este equipo determina que el incidente tiene un mayor impacto o no puede ser resuelto adecuadamente, puede ser reclasificado como Nivel 3, lo que activa el Procedimiento de Gestión de Crisis, involucrando al Comité de Seguridad. En todos los casos se documentan las acciones realizadas, se analiza la causa raíz, se generan informes y se concluye con una propuesta de cierre que será validada antes del cierre definitivo del incidente.

6.4.2 Flujo resolución de incidencias Nivel 1 y Nivel 2



El procedimiento comienza cuando se confirma un incidente de seguridad de la información. El **Encargado de Seguridad de la Información (ESI)** activa la **respuesta inmediata** y clasifica el incidente según su prioridad. Si es de Nivel 1 (baja o media), se asigna directamente a la unidad resolutora; si es de Nivel 2 (alta), se deriva al **Equipo de Respuesta a Incidentes (ERI)**. A continuación, se registra el incidente en el sistema y se aplican medidas de contención y corrección. Una vez alcanzada la recuperación funcional, se ajusta la documentación técnica y se solicita aprobación de cierre a ESI o al ERI, según corresponda. Si la solución es rechazada, se inicia un ciclo de revisión y reingreso del incidente para su reevaluación.

En casos donde el incidente implica una condición que requiere crear o modificar procedimientos, el ERI evalúa su necesidad. Si procede, se desarrolla un procedimiento preliminar que deberá ser aprobado. Si se detecta un aumento de severidad o riesgo a futuro que exceda las capacidades del Nivel 2, se notifica al **Comité de Seguridad**, lo que puede escalar el caso a Nivel 3. Una vez validada la solución, se procede con la aprobación del ESI y se notifican a las partes interesadas. Finalmente, se genera el informe de cierre y se formaliza el cierre del incidente.

6.4.3 Registro y Clasificación del Incidente.

- ✓ **Registro Incidente Inicial (Mesa de Servicio TI)**
  - ✓ **Funcionario:**
  - ✓ Asunto
  - ✓ Categoría: Seguridad -> Incidentes de Seguridad
  - ✓ Descripción
- ✓ **Clasificación:**
  - ✓ **Encargado de Seguridad de la Información:**
  - ✓ Origen: Portal, Teléfono, Correo Electrónico, Slack, Lugar de Trabajo
  - ✓ Tipo: Incidente
  - ✓ Urgencia: Bajo, Medio, Alto
  - ✓ Impacto: Bajo, Medio, Alto
  - ✓ Estado: Abierto
  - ✓ Grupo: Gestores de Seguridad TI (siempre que el funcionario categorizara correctamente)
  - ✓ Agente: Selección según disponibilidad
  - ✓ Departamento: Estructura Orgánica Hospital de Tomé
  - ✓ Categoría: Seguridad -> Incidentes de Seguridad
  - ✓ Tipo de Incidente Seguridad: Informático / No Informático

El Agente asignado que para este caso será generalmente el ESI, podrá hacer uso de las siguientes secciones:

- ✓ **Conversaciones:**
  - ✓ Responder
  - ✓ Reenviar
  - ✓ Agregar Nota (Pública o Privada)
- ✓ **Tickets Relacionados**
  - ✓ Agregar Ticket relacionados
- ✓ **Tareas**
  - ✓ Agregar Tareas (Cada Tarea tiene un Subconjunto de Datos)
  - ✓ Cambiar Estados de Tareas
- ✓ **Aprobaciones**
  - ✓ El ESI podrá solicitar aprobaciones cuando corresponda, esto es muy útil cuando se necesita validar información.
- ✓ **Resolución**
  - ✓ Cuando el incidente este superado, es obligatorio indicar una Resolución.

Una vez que el ESI realizase la Evaluación del incidente y recopilara toda la información necesaria.

6.4.4 Tipo de Incidente.

Tipo	Descripción	Ejemplos
a) Informático	Todos aquellos incidentes que afecten las tecnologías de la información o continuidad de las operaciones	▪ Denegación de servicios computacionales ▪ Fallas del sistema de información ▪ Código malicioso ▪ Accesos no autorizados a los sistemas de información ▪ Infraestructura TIC
b) No informático	Todos aquellos incidentes no contemplados en el punto anterior	▪ Violaciones a la confidencialidad, integridad y disponibilidad (documento) ▪ Filtración de información reservada ▪ Incidentes provocados por la naturaleza ▪ Acceso físico no autorizado

6.4.5 Incidente Grave

Cuando el ESI realizase la Evaluación del incidente y confirmase que se trata de un incidente de seguridad de la información cualquiera fuese su nivel (Prioridad Baja, Media, Alta, Urgente) se debe crear un Incidente Grave en la plataforma de gestión de incidentes y completar los siguientes campos:

- ✓ Solicitante
- ✓ Asunto
- ✓ Incidente de Servicio (Corte Total / Corte Parcial / Degradación de Servicios)
- ✓ Impacto de Negocio
- ✓ Locaciones Impactadas
- ✓ N° de Afectados
- ✓ Origen (Teléfono / Correo / Portal / Slack / Lugar de Trabajo)
- ✓ Estado, inicialmente estará en "Abierto"
- ✓ Urgencia (Alto / Medio / Bajo)
- ✓ Impacto (Alto / Medio / Bajo)
- ✓ Prioridad (Bajo, Medio, Alto, Urgente)
- ✓ Grupo, generalmente será "Gestores de Seguridad TI", pero podría establecerse directamente "Equipo de Respuesta de Incidentes"
- ✓ Agente, Será el ESI.
- ✓ Departamento (Lugar de afectación)
- ✓ Categoría (Tipo de Activo)

- ✓ Tipo de Incidente (Informático / No Informático)
- ✓ Descripción
- ✓ Asociar Activo, no es obligatorio, sin embargo, es deseable que se indique el activo o servicio afectado.

La formulación de este "Incidente Grave" en la plataforma de gestión de incidente institucional es debido a que ofrece un nivel de gestión mayor respecto al "Incidente", permitiendo flujos internos con un mayor detalle.

Una vez que se cree el Incidente Grave el gestor o gestores del mismo podrán actualizar el estado de infraestructura si fuese necesario lo que gatillara procesos internos de notificaciones a las partes interesadas y se reflejará en el Portal de Estado de Infraestructura TI. Para lo anterior es importante que el responsable siga la evolución natural del incidente a través de los estados propuestos.

Es imperativo que las actualizaciones se realicen al menos cada 30 minutos a menos que se indique expresamente por alguna tercera una cronología de actualización.

6.4.6 Nivel de criticidad.

Una vez que se recibe la información sobre las causas del incidente, identifica alternativas de solución y, en caso de que la solución implique costos, se debe cuantificarlos para gestionar su aprobación.

Asimismo, deberá registrarse la información recopilada (Anexo N°1), descripción, responsables, análisis de la ocurrencia del incidente, tiempo de respuesta y solución al incidente, finalmente cuantificar y monitorear el tipo, volumen y costo del incidente. En caso de que haya implicancias legales o de otro tipo, deberá poner antecedentes en conocimiento de la División Jurídica y jefe de servicio para acordar curso a seguir. Toda respuesta a eventos y/o incidentes significativos deberá al menos incluir los siguientes aspectos para un mejor desempeño y atención del incidente:

- Recopilar la evidencia lo más pronto posible después de la verificación;
- Clasificar el Incidente de acuerdo con su tipo de taxonomía: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
- Clasificar la severidad (Prioridad) del incidente de acuerdo con la siguiente tabla:

N°	Nivel	Descripción
1	Bajo	Impacto bajo sobre los activos: daño desde la amenaza no tiene consecuencias relevantes.

2	Medio	Impacto medio sobre los activos: daño desde la amenaza tiene consecuencias importantes.
3	Alto	Impacto alto sobre los activos: daño desde la amenaza tiene consecuencias graves sobre los activos.
4	Urgente	Impacto muy alto o Urgente: daño desde la amenaza tiene consecuencias catastróficas sobre los activos.

- Efectuar escalamiento Nivel 2 (Equipo Respuesta Incidentes), según la pertinencia y relevancia del incidente;
- Asegurarse de que todas las actividades de respuesta se registren correctamente para el posterior análisis;
- Comunicación de la existencia del incidente de seguridad de la información o cualquier detalle pertinente a otras personas u organizaciones internas o externas que deban ser informadas o advertidas sobre estos incidentes;
- Manejar las debilidades de la seguridad de la información que causan o contribuyen al incidente;

6.4.7 Análisis y Evaluación de un Incidente de Seguridad Nivel 2 (Evaluación 2)

En el caso de que el incidente sea considerado por el evaluador (ESI) nivel 2 (Alto) como incidente relevante, este deberá realizar las siguientes actividades:

- Analizar toda la información relevante recopilada.
- Validar o reclasificar la severidad del incidente de acuerdo con la siguiente tabla:

N°	Nivel	Descripción
1	Bajo	Impacto bajo sobre los activos: daño desde la amenaza no tiene consecuencias relevantes.
2	Medio	Impacto medio sobre los activos: daño desde la amenaza tiene consecuencias importantes.
3	Alto	Impacto alto sobre los activos: daño desde la amenaza tiene consecuencias graves sobre los activos.

N°	Nivel	Descripción
4	Urgente	Impacto muy alto o Urgente: daño desde la amenaza tiene consecuencias catastróficas sobre los activos.

- Gatillar Respuesta Inmediata.
- Iniciar cadena de custodia.
- Realizar análisis forenses de seguridad de la información, según sea necesario;
- Ejecutar Plan de Comunicaciones Interna.
- Documentar el incidente.
- Una vez que se ha manejado el incidente correctamente, se deberá cerrar y registrar formalmente.

Este nivel establecerá los procedimientos de respuesta específicos que permitan de una manera ordenada, estandarizada, segura y eficaz, responder a estas anomalías en la seguridad institucional.

Todos los incidentes de seguridad, incluyendo los falsos positivos, que hayan sido evaluados por el nivel 2 deberán ser revisados mediante análisis post-incidente, para identificar el origen de este, sus posibles implicancias, impacto en la organización, estudio de tendencias de incidentes analizados, así como también con el propósito de realizar una mejora continua sobre las acciones de control realizadas por esta unidad.

En caso de que el incidente de seguridad sea considerado relevante (Nivel de severidad 2 - Alto) y no haya podido ser resuelto, es decir, que el incidente pese al plan de respuesta inmediata aplicado NO esté bajo control, deberá activarse el Proceso de Gestión de Crisis en conjunto con el Comité de Seguridad de la Información.

6.4.8 Respuesta Inmediata.

El responsable del o los activos involucrados designados para la respuesta inmediata del incidente es o son responsables del desarrollo de las siguientes acciones inmediatas:

Actividad	Descripción
Contener el daño y minimizar el riesgo	Evitar que se propaguen los daños o efectos del incidente, coordinando las actividades necesarias para su disminución, probabilidad y consecuencia.

Actividad	Descripción
Reclasificar el incidente si fuera necesario	Reclasificar según punto 6.4.5
Protección de evidencias	Resguardar las evidencias recopiladas durante la gestión.
Notificación a los organismos externos	Cuando sea necesario notificar a organismos externos como por ejemplo (carabineros, PDI, Bomberos, etc.).
Recuperación de los sistemas	Contactar al administrador de el o los sistemas a fin de gestionar la recuperación de éstos.
Escalar con proveedores externos	Contactar a los proveedores expertos en el Activo Vital y en conjunto con ellos se deberá gatillar el plan de acción para resolver el incidente a la brevedad posible.
Compilación y organización de la documentación del incidente	Recopilar todos los antecedentes relacionados con el incidente.

En esta etapa el Encargado de Seguridad de la Información debe entregar lineamientos para la respuesta ante un incidente.

6.4.9 Activación de resolución de incidencias Nivel 3.

Si un incidente se agrava en su nivel de severidad o impacto en las personas o procesos, la propiedad y la infraestructura (Activos Institucionales Vitales), y que además sea probable que continúe por un tiempo más prolongado de lo previsto, se entiende que este incidente pasa a ser una crisis y tratado de acuerdo con la siguiente organización.

6.5 Equipo de respuesta a incidentes y Comité de Seguridad.

El equipo de respuesta a Incidentes y el Comité de Seguridad serán los responsables de la gestión de los Incidentes dentro de la organización. Sus principales responsabilidades son: acelerar los procesos para la toma de decisiones en la resolución de incidentes, definir las prioridades, establecer la estrategia, asignar recursos y táctica a seguir.

Este es presidido por la figura máxima con capacidad de decisión (responsable máximo del organismo y/o representante del Gabinete de Ministro/a o Subsecretarios/as. Junto con ello

debe tener representación y subrogante de a lo menos las siguientes áreas del Organización: Encargado de Seguridad de la Información y Ciberseguridad, RRFF, TIC (Jefe TI, Operaciones TI, Tecnologías Digitales), Dueños de los Procesos, Recursos Humanos, Finanzas, Jurídica y Comunicaciones. La gestión de crisis no es algo exclusivo del equipo de seguridad o tecnología, sino que implica a toda la organización, bajo este concepto a este equipo se puede invitar a subdirectores.

Será el presidente del comité el responsable de definir si se está ante una crisis o no, su nivel de criticidad, definición de medidas y asignación de responsabilidades, así como los distintos responsables en cada caso, desde lo operativo para la contención y resolución del incidente, hasta la coordinación y comunicación que velará por la imagen de la institución, estableciendo la política de información, con los comunicados más adecuados y canales oportunos.

A continuación, se presenta un cuadro resumen de los actores del Comité de Seguridad y sus responsabilidades:

Representante	Responsabilidades
Presidente	▪ Inicia la gestión de crisis y preside el comité de seguridad. ▪ Delega responsabilidades. ▪ Se mantiene permanentemente informado. ▪ Actúa como portavoz si las circunstancias lo exigen.
Encargado de Ciber/Seguridad de la Información	▪ Es el primero en conocer el incidente y debe determinar nivel de criticidad (Impacto y Urgencia), si es preciso trasladarlo o no al comité de Seguridad. ▪ Notifica al CSIRT / ANCI de referencia. ▪ Determina cuáles son las primeras acciones operativas para su contención.
TIC	▪ Gestiona la continuidad de los servicios, utilizando según sea el caso, los respaldos o sitios de contingencia para los servicios críticos. ▪ Revisa el entorno común de todas las aplicaciones (comunicaciones, firewall, DNS, etc..), así como los específicos de cada aplicación. ▪ Gestionará de forma rápida servidores virtuales en caso de ser necesario. ▪ Activar Política de copias de seguridad.
Jurídica	▪ Determina las responsabilidades legales directas provocadas por el incidente. ▪ Da seguimiento a las acciones a seguir de acuerdo a la leyes y normas aplicables.

Representante	Responsabilidades
	▪ Orienta sobre todos los asuntos legales.
Comunicaciones	▪ Integra el Comité de Seguridad y adopta el Manual de comunicaciones de crisis previamente elaborado. ▪ Decide cuáles son los mensajes clave, el formato y canal más adecuado, en función de los grupos de interés. ▪ Activa el seguimiento y percusión de la crisis en los diferentes medios de comunicación y redes sociales. ▪ Mantiene contacto con los medios de comunicación.
Administración y Finanzas **RRFF**	▪ Analiza los recursos necesarios para la resolución de la crisis. ▪ Recopila información, evalúa los hechos y plantea opciones. ▪ Mantiene comunicación con las compañías aseguradoras (si aplica).
Recursos Humanos **(se extiende a SDM – Gestión del Cuidado)**	▪ Portavoz ante los funcionarios y en caso de ser aplicable, los representantes. ▪ Gestiona las acciones operativas en caso de incidentes relacionados con personas. ▪ Comunica, llegado el caso, con los afectados y facilita información o asistencia básica (por ejemplo, en caso de una lesión de un funcionario). ▪ Evalúa el ánimo de los funcionarios y recomienda acciones para evitar decaimiento o una evolución no prevista.

6.6 Declaración del Nivel de crisis y equipo responsable según el nivel de criticidad (Impacto y Urgencia):

Atributo	Nivel de criticidad			
	Bajo	**Medio**	**Alto**	**Urgente**
Declaración de Crisis	NO	NO	OPCIONAL	SI
Nivel	1	1	2	3
Ámbito de Gestión /Gobierno de crisis	No requiere comité de Seguridad Responde equipo Operativo - ESI	No requiere Comité de Seguridad Responde Encargado Área TIC, ESI y Negocio	Opcional Comité de Crisis según ESI Preside ESI Equipo de Respuesta Incidente	Requiere Comité de Crisis Preside Representante Dirección
Procedimiento	PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			PROCEDIMIENTO GESTIÓN DE CRISIS

Ante incidentes con peligrosidad baja y media no deberían requerir la convocatoria de un Comité de Seguridad, porque no se encuentra ante una situación que se pueda definir como tal.

Bajo la responsabilidad directa del Encargado de Ciberseguridad, los equipos técnicos tienen el conocimiento para solucionar el problema en el nivel operativo.

6.7 Proceso Disciplinario.

Si el incidente es de mayor gravedad o se sospecha la comisión de algún delito, el Comité de Seguridad de la Información, asesorándose por el integrante de la Unidad jurídica designada para las materias de Seguridad de Información, informará al Jefe Superior del Servicio y, de precisarse, a carabineros, bomberos, ambulancias, Ministerio Público, etc.

En el caso que existan eventuales responsabilidades administrativas, y dependiendo de la gravedad del incidente, el Comité de Seguridad de la Información solicitará a quien corresponda la instrucción de un procedimiento disciplinario para la investigación de las eventuales responsabilidades en los términos previstos en el Estatuto Administrativo.

Cuando el incidente involucre a personal contratado a honorarios o terceros, se evaluará solicitar el término anticipado del contrato o, en caso de que exista, la aplicación de la

sanción que establezca el propio contrato, Política General de Seguridad de la Información u otras políticas ministeriales para el incidente detectado.

6.8 Continuidad de la Seguridad de la Información.

En caso de que el incidente no pueda ser controlado y ponga en riesgo las operaciones y entrega de productos y servicios del Ministerio, el Comité de Seguridad de la Información, evaluará la activación de los procesos de continuidad del negocio.

6.9 Recolección de evidencia.

La recolección de la evidencia es responsabilidad del responsable del activo involucrado, designado para la resolución del incidente, la que debe ser reportada al Encargado de Seguridad para su revisión, ésta debe ser clara y suficiente. Para ello se deberá:

- Para los documentos en papel:
  - ✓ Se debe levantar inventario de los documentos.
  - ✓ El original es incluido en la cadena de custodia, y se guarda de manera segura con un registro del individuo que encontró el documento, dónde y cuándo fue encontrado el documento, y quién fue testigo del descubrimiento. En cualquier investigación se debe asegurar que los originales no son alterados.
  - ✓ Para los análisis se utilizarán copias numeradas de circulación controlada.

- Para la información sobre medios computacionales:
  - ✓ El proceso se inicia con la generación de una imagen espejo en presencia del ministro de fe de la institución. Se levanta inventario y se inicia la cadena de custodia.
  - ✓ El o los archivos originales y copias espejo se deben guardar de manera segura e intactos (se utilizan mecanismos de protección e incluso encriptación para que nadie adultere la evidencia).
  - ✓ En el caso de que no sea factible aislar y sacar de producción el original, la copia 1 será considerada original a estos efectos, en la medida que se resguarde el procedimiento anterior.
  - ✓ Las imágenes o copias espejo (dependiendo de los requisitos aplicables) de cualquier medio removible, información en discos duros o en memorias, deben ser numeradas y retenidas para asegurar su disponibilidad.
  - ✓ De todas las operaciones de análisis sobre estas copias se levantará acta identificando las personas que las manipulan, detalle de las operaciones realizadas y sus hallazgos o resultados.

- ✓ El registro de todas las acciones durante el proceso de copiado se debería guardar y el proceso se debería efectuar ante testigos.

Cualquier trabajo forense se debe realizar sólo sobre copias del material de evidencia. Se debe supervisar y registrar cuándo y dónde fue ejecutado el proceso de copiado, quién realizó las actividades de copiado y qué herramientas y programas se han utilizado.

Si corresponde esta evidencia debe ser entregada al Comité de Seguridad de la Información para la evaluación de procesos disciplinarios.

6.10 Comunicación a los involucrados.

Una vez contenido el incidente, el Encargado de Seguridad de la Información debe informar a los involucrados en el Incidente.

6.11 Análisis de causa y cierre del incidente.

En esta etapa el Responsable del activo, designado para la resolución del incidente debe:

- Realizar un análisis de las causas del Incidente.
- Cuando el incidente no esté cerrado, seleccionar e implementar un plan de acción adecuado, además de definir el plazo para su implementación, dejando registro de las actividades. El seguimiento de este plan será responsabilidad del Encargado de Seguridad de la Información.
- Registrar el cierre del Incidente en un informe de cierre del incidente. (Obligatorio)

6.12 Aprender de los incidentes en la seguridad de la información

A lo menos cada 12 meses el Encargado de Seguridad de la Información, debe revisar los incidentes de seguridad del período analizando:

- Posibles tendencias.
- Eficacia de los tratamientos implementados.
- Cuantificación de los tipos, volúmenes y costos de los incidentes de seguridad.
- Incidentes recurrentes o de alto impacto.
- Problemas subyacentes y medidas correctivas desarrolladas.
- Necesidades de mejorar o implementación de nuevos controles para limitar la frecuencia, daño y costo de futuras ocurrencias.

Con los antecedentes aportados por esta revisión, el Encargado de Seguridad de la Información debe proponer al Comité de Seguridad de la Información medidas que sean necesarias para que no vuelvan a ocurrir, además de detectar y promover los aprendizajes de cada uno de ellos.

7 PLAZOS DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.

De acuerdo con lo establecido en la Ley N° 21.663, Ley Marco de Ciberseguridad, se deben reportar al CSIRT Nacional los incidentes de ciberseguridad o ciberataques que puedan tener efectos significativos.

Todo incidente de seguridad debe ser notificado dentro de los siguientes plazos:

- Dentro de las 3 horas siguientes a conocer el incidente, se debe enviar una alerta temprana.
- Dentro de las 72 horas, se debe enviar una actualización con la evaluación inicial del incidente, su gravedad e impacto.
- Dentro de los 15 días corridos, se debe enviar un informe final sobre el incidente y las medidas adoptadas.

Nota: Se deberán informar a CSIRT Nacional aquellos Incidentes que provoquen la interrupción de la continuidad de un servicio esencial, afectar la integridad física o la salud de las personas, afectar sistemas informáticos que contengan datos personales.

El incumplimiento de estos plazos será considerado una falta grave, de conformidad con las normativas internas y los estándares legales, y podrá derivar en acciones disciplinarias o contractuales según corresponda.

8 REGISTROS:

- Registros cadena de custodia
- Registro de análisis de incidentes.
- Registro de gestión de vulnerabilidades.
- Acta de análisis de hallazgos
- Planilla registro de incidentes.
- Plan de acción.
- Informe de incidentes.
- Registro de cumplimiento del deber de notificar incidente
- Registro de cumplimiento de obligación de denuncia (si procede)
- Registro de Evidencias.

9 DIFUSION:

La comunicación del presente procedimiento se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Portal Mesa de Servicio TI, sección Ayuda, Seguridad.
- Correo informativo.

10 PERÍODO DE REVISIÓN.

El presente procedimiento deberá ser revisado cada dos años o cuando ocurran cambios significativos para garantizar que:

- Sigue siendo adecuado para su propósito y preciso.
- Refleja los cambios en las tecnologías.
- Está alineado con la legislación vigente, los estándares internacionales y las mejores prácticas.

11 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA.

En situaciones excepcionales, el Jefe de Área TIC, el CISO o el Comité de Seguridad de la Información tendrán la facultad de evaluar y establecer condiciones específicas para la excepción al cumplimiento de las directrices establecidas en esta política, siempre que tales excepciones no infrinjan la legislación vigente ni comprometan la seguridad de la información.

Cada excepción deberá ser debidamente documentada, y se deberá iniciar un proceso de revisión de la política en el que se determinará si es necesario incorporar directrices adicionales o realizar modificaciones específicas.

12 CONTROL DE VERSIONES:

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
1			

13 ANEXOS

Anexo 1: Datos mínimos que deben ser registrados en el informe de incidentes.

VARIABLE	DESCRIPCIÓN
Prioridad	CAPS. Prioridad del incidente
Impacto	CAPS. Valoración del Impacto del Incidente
Brecha de SLA	CAPS. Evaluación de cumplimiento de SLA
Incidente Grave Asociado	CAPS. Identificación del Incidente Base asociado
Tipo de Incidente Grave	CAPS. Identificación del tipo de Incidente Grave
N° Funcionarios Afectados	CAPS. Cantidad de funcionarios afectados por Incidente
Locaciones Impactadas	CAPS. Cantidad de locaciones afectadas
Impacto de Negocio	CAPS. Descripción del Impacto para el Negocio
Servicios Impactados	CAPS. Lista de servicios impactados en el Incidente
Asignado a	CAPS. Agente asignado al Incidente
ESI del Incidente Grave	MANUAL. Nombre del ESI a cargo
Grupo	CAPS. Grupo asignado a la resolución del Incidente
Respondedores	CAPS. Grupo de personas asignadas para responder
Estado	CAPS. Estado del Incidente
Origen	CAPS. Origen de la creación del Incidente
Se Activa Cont. Negocio	MANUAL. Dato booleano para identificar Cont. Negocio
Tipo de Incidente	CAPS. Identificación de tipo Informático / No Informático

*CAPS: Campo Autocompletado por el Sistema

Cronología del Incidente:

VARIABLE	DESCRIPCIÓN
Creación del Incidente	CAPS
Escalado a Incidente Grave	CAPS
Agente Conoce Incidente	CAPS
Resolución de Incidente	CAPS
Tiempo Medio de Detección	CAPS
Tiempo Medio de Reconocimiento	CAPS
Tiempo medio de Resolución	CAPS
Duración Total de Incidente	CAPS

*CAPS: Campo Autocompletado por el Sistema

Resumen del Incidente

VARIABLE	DESCRIPCIÓN
Síntomas Observados	Semi CAPS, se debe completar.
Análisis Causa Raíz	Apartado de investigación de Causa Raiz.
Impacto	Detalle de Impacto de Incidente
Pasos Diagnósticos	Enumeración de cada paso para determinar el diagnóstico del incidente.
Pasos de Resolución	Enumeración de cada paso para determinar la Resolución del Incidente.
Pasos Preventivos	Enumeración de cada paso preventivo utilizado durante el Incidente.

Acciones Realizadas.

En esta sección se deben indicar todas las tareas realizadas durante el incidente, para ello es recomendable utilizar el modulo de tareas del sistema de gestión de incidencias. Las variables a completas son:

VARIABLE	DESCRIPCIÓN
ID Tarea	ID de Tarea del Sistema de Gestión de Incidencias
Tarea	Nombre de la Tarea
Asignación	Agente Asignado o Grupo
ETA	Tiempo transcurrido en la ejecución de la Tarea.

Incidentes Relacionados

Sección donde se indicarán los incidentes en sistema que puedan tener relación con el evento mayor (Incidente Grave)