Servicio de Salud Tarapacá
Ministerio de Salud
Gobierno de Chile

Servicio de Salud Tarapacá
Hospital Dr. Ernesto Torres G.
ACS/PAIC/FPS/JVD/CRR/EOM/FAV/fcs

APRUEBA INSTRUCTIVO DE CIBERSEGURIDAD E INSTRUYE SU APLICACIÓN PARA EL HOSPITAL DR. ERNESTO TORRES GALDAMES.

RESOLUCIÓN EXENTA Nº 1325 /

IQUIQUE, 29 MAY 2025

VISTOS

Estos antecedentes, Ley N° 18.575, de 1986 del Ministerio del Interior, Orgánica Constitucional de Bases Generales de la Administración del Estado; D.F.L. N° 1, de 2005, del Ministerio de Salud, Fija texto refundido, coordinado y sistematizado del Decreto Ley N° 2.763, de 1979 y de las Leyes N° 18.933 y N° 18.469; Ley N° 19.937, de 2004 que modifica el Decreto Ley N° 2.763, de 1979 con la finalidad de establecer una nueva concepción de la Autoridad Sanitaria, distintas modalidades de gestión y fortalecer la participación ciudadana; Ley N° 19.880, de 2003 del Ministerio Secretaria General de la Presidencia, Establece Bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; Decreto N° 140, de 2004, del Ministerio de Salud, que Aprueba Reglamento Orgánico de los Servicios de Salud; D.F.L. N° 29, de 2004 del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834 sobre Estatuto Administrativo; Decreto Afecto Nº56, de 2022 del Ministerio de Salud; Ley Nº20.766, de 2014 del Ministerio Secretaría General de la Presidencia, Establece Procedimiento de Toma de Razón y Registros Electrónicos; Ley N° 19.799 sobre documentos electronicos, forma electronica y servicios de certificación de dicha firma; el Decreto Supremo N° 83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; Ley N° 19.233 sobre delitos informaticos; Ley Nº 21.663 Marco de Ciberseguridad; Norma Chilena NCh-ISO 27001:2013 Tecnología de la información, Técnicas de seguridad - Sistemas de gestión de la seguridad de la información, las Resoluciones Nº18, de 2017 y Nº06, de 2019, de la Contraloría General de la República; la Resolución Exenta N° 1.763 de fecha 08.08.2024 que crea el Comité de Ciberseguridad del Hospital Dr. Ernesto Torres Galdames, la Resolución Exenta N° 2.712 de fecha 30.12.2024 que aprueba la Política General de Seguridad de la Información y Ciberseguridad para el Hospital Dr. Ernesto Torres Galdames y las facultades que me otorga la Resolución Exenta N° 4.870 de fecha 13.11.2024 del Servicio de Salud de Tarapacá.

CONSIDERANDO:

Que, en el tenor de la Ley Marco de Ciberseguridad Nº 21.663 y la Política Nacional de Ciberseguridad 2023-2028, es imperativo incorporar en la gestión un Instructivo de Ciberseguridad para el Hospital Dr. Ernesto Torres Galdames.

Que, el instructivo se genera a partir del programa de actividades, compromisos y acuerdos del Comité de Ciberseguridad del Hospital Dr. Ernesto Torres Galdames, los integrantes del citado Comité concurren son sus firmas en el Instructivo.

Que, el Instructivo de Ciberseguridad nace en el marco de la Política General de Seguridad de la Información y Ciberseguridad para el Hospital Dr. Ernesto Torres Galdames aprobada mediante la Resolución Exenta N° 2.712 de fecha 30.12.2024,

RESUELVO:

1° APRUÉBESE el ***Instructivo de Ciberseguridad*** del Hospital de Iquique Dr. Ernesto Torres Galdames, adjunto en anexo "A".

2° DECLÁRESE el ***Instructivo de Ciberseguridad*** del Hospital Dr. Ernesto Torres Galdames de Iquique, a contar del mes de mayo del año 2025, con una duración de dos años, hasta el mes de mayo del año 2027.

3° ESTABLÉZCASE el ***Instructivo de Ciberseguridad*** del Hospital Dr. Ernesto Torres Galdames de Iquique que se acompaña a la presente Resolución como parte íntegra de esta.

4º PUBLÍQUESE el ***Instructivo de Ciberseguridad*** del Hospital Dr. Ernesto Torres Galdames de Iquique en banner dedicado a estos fines de la página web institucional.

5º DÉSE amplia difusión, promuévase y aplíquese el *Instructivo de Ciberseguridad,* para proteger la confidencialidad, integridad y disponibilidad de toda la información que maneja, especialmente los datos de los pacientes. Este instructivo establece las pautas y obligaciones que todo el personal debe seguir para garantizar la seguridad de la información y los sistemas del hospital.

6° INSTRÚYASE, a todas las y los funcionarios, Unidades y Servicios Clínicos, Unidades Asesoras y Administrativas del Hospital Dr. Ernesto Torres Galdames, a la aplicación y sujección del ***instructivo*** que se indica en los puntos precedentes y que forma parte íntegra de la presente resolución.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE, ARCHÍVESE.

HOSPITAL DR. E.TORRES G. DIRECTOR IQUIQUE

DR. ALDO CAÑETE SOTO
DIRECTOR (S)
HOSPITAL "DR. ERNESTO TORRES GALDAMES"

Lo que me permito transcribir a Ud., para su conocimiento y fines pertinentes.

HOSPITAL DR. E.TORRES G. MINISTRO DE FE IQUIQUE

MINISTRO DE FE
BERNARDITA JORQUERA GARCÍA

DISTRIBUCIÓN
- Dirección HDETG sec.director.hetg@redsalud.gob.cl
- Dirección SST director.ssi@redsalud.gob.cl
- Subdirección Médica HDETG sdm.hetg@redsalud.gob.cl
- Subdirección Gestión Cuidado de Paciente HDETG sdgcp.hetg@redsalud.gob.cl y fernando.pacheco@redsalud.gob.cl
- Subdirección Administrativa HDETG secretariasda.hetg@gmail.com cristian.palacios@redsalud.gob.cl
- Subdirección de Gestión y Desarrollo de las Personas HDETG juancarlos.vega@redsalud.gob.cl
- Departamento de Informática eric.ossandon@redsalud.gob.cl
- Unidad de Grupo Relacionado a Diagnóstico (GRD) cristian.rojas.p@redsalud.gob.cl
- Unidad de Planificación y Control de la Gestión Hospitalaria fresia.amas@redsalud.gob.cl y ccgestionhetg@gmail.com
- Unidad de Estadísticas y Gestión de la Información en Salud patricio.chandia@redsalud.gob.cl
- Unidad Asesoría Jurídica juridicahospitaliquique@gmail.com
- Unidades Asesoras de Dirección.
- Funcionario encargado de RISPAC gerardo.gemio@redsalud.gob.cl
- Unidades Administrativas.
- Unidades y Servicios Clínicos.
- Oficina de Partes oficina.partes.hetg@gmail.com

RESUELVO:

1° APRUÉBESE el ***Instructivo de Ciberseguridad*** del Hospital de Iquique Dr. Ernesto Torres Galdames, adjunto en anexo "A".

2° DECLÁRESE el ***Instructivo de Ciberseguridad*** del Hospital Dr. Ernesto Torres Galdames de Iquique, a contar del mes de mayo del año 2025, con una duración de dos años, hasta el mes de mayo del año 2027.

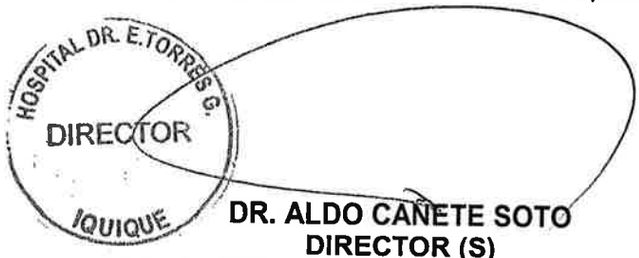
3° ESTABLÉZCASE el ***Instructivo de Ciberseguridad*** del Hospital Dr. Ernesto Torres Galdames de Iquique que se acompaña a la presente Resolución como parte íntegra de esta.

4º PUBLÍQUESE el ***Instructivo de Ciberseguridad*** del Hospital Dr. Ernesto Torres Galdames de Iquique en banner dedicado a estos fines de la página web institucional.

5º DÉSE amplia difusión, promuévase y aplíquese el *Instructivo de Ciberseguridad*, para proteger la confidencialidad, integridad y disponibilidad de toda la información que maneja, especialmente los datos de los pacientes. Este instructivo establece las pautas y obligaciones que todo el personal debe seguir para garantizar la seguridad de la información y los sistemas del hospital.

6° INSTRÚYASE, a todas las y los funcionarios, Unidades y Servicios Clínicos, Unidades Asesoras y Administrativas del Hospital Dr. Ernesto Torres Galdames, a la aplicación y sujección del ***instructivo*** que se indica en los puntos precedentes y que forma parte íntegra de la presente resolución.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE, ARCHÍVESE.



DR. ALDO CAÑETE SOTO
DIRECTOR (S)
HOSPITAL "DR. ERNESTO TORRES GALDAMES"

INSTRUCTIVO DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN HOSPITAL DR. ERNESTO TORRES GALDAMES

Introducción

El Hospital de Iquique Dr. Ernesto Torres Galdames se compromete a proteger la confidencialidad, integridad y disponibilidad de toda la información que maneja, especialmente los datos de nuestros pacientes. Este instructivo establece las pautas y obligaciones que todo el personal debe seguir para garantizar la seguridad de la información y los sistemas del hospital. El cumplimiento de estas normas es esencial para prevenir incidentes de seguridad, proteger la privacidad de los pacientes y mantener la confianza en nuestros servicios.

1. Reporte de Actividades Sospechosas

- **Obligación de informar:** Todo el personal tiene la obligación de informar de inmediato al Departamento de Informática sobre cualquier correo electrónico, mensaje o actividad que parezca sospechosa o maliciosa.
  - **Justificación:** Esto permite una respuesta rápida ante posibles amenazas, como phishing o malware, reduciendo el riesgo de daños.
- **Pérdida de información:** Se debe informar a la jefatura directa y al Departamento de Informática sobre cualquier conocimiento de pérdida, robo o divulgación no autorizada de información estratégica de la institución.
  - **Justificación:** Permite activar los protocolos de respuesta a incidentes y minimizar el impacto de la pérdida de información.

2. Uso Adecuado de los Recursos Informáticos

- **Prohibición de borrar información:** Está prohibido borrar información de los equipos computacionales de la institución sin la autorización correspondiente.
  - **Justificación:** Esto asegura la integridad de los datos y facilita la trazabilidad de las acciones realizadas en los sistemas.
- **Conexión de dispositivos personales:** Se prohíbe conectar dispositivos personales, como teléfonos celulares, tablets u otros, a los equipos computacionales de la institución, incluso para la carga.
  - **Justificación:** Esto reduce el riesgo de introducir malware o virus a la red del hospital y protege la información confidencial.
- **Descarga de software no autorizado:** Se prohíbe descargar o instalar software no autorizado en los dispositivos de la institución.
  - **Justificación:** El software no autorizado puede ser malicioso o incompatible con los sistemas del hospital, lo que puede comprometer la seguridad y la estabilidad de la red.
- **Descarga de software de VPN:** Se prohíbe descargar o instalar software no autorizados de VPN, túneles informáticos o cualquier otra herramienta que pueda comprometer o saltar las reglas de seguridad establecidas para la red informática del Hospital de Iquique.
  - **Justificación:** El software no autorizado puede ser malicioso o incompatible con los sistemas del hospital, lo que puede comprometer la seguridad y la estabilidad de la red.
- **Compartir datos móviles personales:** Se prohíbe compartir datos móviles personales en los dispositivos de la institución.
  - Justificación: Esta acción puede abrir brechas de seguridad en la red hospitalaria, facilitando el acceso no autorizado a información sensible.
- **Uso de internet privada:** Se prohíbe usar señal de internet privada desde equipos telefónicos, enrutadores (routers) u otros dispositivos privados en equipos computacionales, equipos clínicos u otros de la institución.

- Justificación: El uso de redes privadas no autorizadas puede exponer los equipos y la información del hospital a riesgos de seguridad externos.

- **Dispositivos de almacenamiento externo:** Se prohíbe el uso de dispositivos de almacenamiento externo (como unidades flash USB, discos duros externos) en equipos computacionales, equipos clínicos u otros de la institución, a menos que sea estrictamente necesario y autorizado por el Departamento de Informática.
  - Justificación: Estos dispositivos pueden ser portadores de malware o facilitar la sustracción de información.
- **Elementos líquidos y comestibles:** Se prohíbe el uso de cualquier tipo de líquido o comestible cerca de los equipos computacionales, equipos clínicos u otros de la institución.
  - Justificación: La presencia de líquidos aumenta significativamente el riesgo de daños irreparables por derrames accidentales en los equipos electrónicos sensibles. Asimismo, el consumo de alimentos puede generar residuos, migas o sustancias pegajosas que pueden contaminar los teclados, ratones y otras partes de los equipos, afectando su funcionamiento y dificultando su limpieza. Restringir estos elementos ayuda a preservar la vida útil de los equipos y a mantener un ambiente de trabajo limpio y seguro.
- **Escritorio limpio:** Se prohíbe dejar a la vista, en escritorio, notas ni en la pantalla del computador información importante (papeles, claves, archivos) cuando no estés.
  - Justificación: Dejar información importante a la vista, ya sea en formato físico (notas, papeles) o digital (claves guardadas, archivos abiertos en pantalla), cuando el usuario se ausenta del puesto de trabajo, incrementa significativamente el riesgo de acceso no autorizado, copia o uso indebido de dicha información por parte de terceros. Esta práctica compromete la confidencialidad y seguridad de los datos institucionales y personales, pudiendo derivar en incidentes de seguridad, robo de identidad o incumplimiento de normativas de protección de datos. La política de escritorio limpio busca mitigar estas vulnerabilidades, promoviendo un ambiente de trabajo seguro y protegiendo la información sensible.

3. Protección de Credenciales y Acceso a la Información

- **Prohibición de compartir contraseñas:** Está estrictamente prohibido compartir contraseñas personales de cualquier sistema o software institucional con otros funcionarios.
  - **Justificación:** Cada funcionario es responsable de las acciones realizadas con sus credenciales. Compartir contraseñas dificulta la trazabilidad y aumenta el riesgo de acceso no autorizado.
- **Responsabilidad de las credenciales:** La responsabilidad y trazabilidad de las acciones realizadas en los sistemas recae en el titular de la cuenta. El consentimiento para compartir la contraseña no exime de esta responsabilidad.
- **Acceso no autorizado a sistemas:** Se prohíbe usar sistemas institucionales para los cuales el funcionario no está autorizado o que no se encuentran dentro de sus tareas y responsabilidades.
  - **Justificación:** Esto asegura que el acceso a la información esté limitado a quienes realmente la necesitan para realizar sus funciones, protegiendo la confidencialidad y la integridad de los datos.
- **Información en correos personales:** Se prohíbe compartir información de la institución, incluyendo datos de pacientes, en correos electrónicos personales.
  - **Justificación:** Los correos electrónicos personales pueden no tener las mismas medidas de seguridad que los sistemas institucionales, lo que aumenta el riesgo de que la información sea interceptada o divulgada.
- **Cierre de sesión:** Se requiere que los funcionarios cierren la sesión de sus cuentas de usuario en los sistemas institucionales (computadores, aplicaciones, plataformas web, etc.) cada vez que se ausenten de su puesto de trabajo, aunque sea por un breve periodo de tiempo, y al finalizar su jornada laboral.
  - **Justificación:** Esto asegura que el acceso a los sistemas y a la información quede restringido al usuario legítimo. Dejar sesiones abiertas permite que personas no autorizadas puedan acceder a las cuentas, visualizar, modificar o sustraer información sensible, realizar acciones en nombre del usuario o comprometer la seguridad de los sistemas institucionales. El cierre de sesión es una medida fundamental para proteger la confidencialidad, integridad y disponibilidad de los datos, previniendo accesos no autorizados y posibles incidentes de seguridad.

4. Manejo de Información Clínica

- **Prohibición de capturas de pantalla y fotografías:** Se prohíbe tomar fotografías o hacer capturas de pantalla de información clínica o exámenes de cualquier tipo.
    - **Justificación:** Esto protege la privacidad del paciente y evita la posible difusión no autorizada de información sensible.
- **Consulta de información clínica:** Se prohíbe consultar información clínica específica si no se es parte del equipo de atención del paciente.
    - Justificación: El acceso a la información clínica debe estar limitado al personal directamente involucrado en la atención del paciente para proteger la privacidad y confidencialidad de los datos.
- **Entrega de información:** Se prohíbe entregar o compartir información clínica o de la institución si no se está habilitado para dicha función o no se encuentra dentro de las responsabilidades del cargo.
    - Justificación: La divulgación no autorizada de información puede tener graves consecuencias legales y éticas, además de dañar la reputación del hospital.

5. Administración de Sistemas

- **Manipulación de sistemas:** Solo el personal del Departamento de Informática está autorizado para manipular los sistemas y las configuraciones de los equipos computacionales o de comunicación de la red informática.
    - **Justificación:** Esto asegura que los sistemas estén configurados y mantenidos de manera segura y que se sigan los procedimientos adecuados.
- **Instalación de Sistemas Informáticos o Software:** Los servicios, unidades o departamentos del Hospital de Iquique que necesiten instalar sistemas informáticos o software para el desarrollo de sus tareas, deberán presentar la solicitud al Comité de CIBERSEGURIDAD, el cual analizará y autorizará dicha acción.
    - Justificación: Este proceso garantiza que cualquier nuevo software o sistema cumpla con los estándares de seguridad del hospital y no represente un riesgo para la red o la información.
- **Manipulación de hardware y periféricos:** Solo el personal del Departamento de Informática está autorizado para manipular hardware y periféricos (equipos PC, mouse, teclados, pantallas, etc,)
    - Justificación: Este proceso garantiza que los componentes informáticos sean debidamente instalados.

6. Gestión de Contraseñas

- **Requisitos de contraseñas:** Todos los funcionarios deben crear contraseñas seguras que cumplan con los siguientes requisitos:
    - Tener una longitud mínima de 12 caracteres.
    - Contener una combinación de letras mayúsculas y minúsculas, números y símbolos.
    - No ser palabras comunes o fácilmente adivinables.
    - No ser reutilizadas.
- **Almacenamiento de contraseñas:** Las contraseñas no deben ser escritas en papel, guardadas en archivos no seguros o compartidas por correo electrónico o mensajería instantánea. Se recomienda utilizar un administrador de contraseñas seguro.
- **Cambio de contraseñas:** Las contraseñas deben cambiarse periódicamente, al menos cada 90 días, y de inmediato en caso de sospecha de compromiso.

7. Uso Seguro del Correo Electrónico

- **Identificación de correos sospechosos:** Se debe tener precaución al abrir correos electrónicos de remitentes desconocidos o que contengan asuntos o enlaces sospechosos.
- **Prevención del phishing:** No se debe hacer clic en enlaces ni descargar archivos adjuntos de correos electrónicos sospechosos. El Hospital de Iquique nunca solicitará información confidencial, como contraseñas o números de identificación, por correo electrónico.

8. Protección contra Malware

- **Software Antivirus:** Todos los equipos deben tener instalado y actualizado un software antivirus aprobado por el Departamento de Informática.

- **Escaneos Periódicos:** Se deben realizar escaneos completos del sistema de forma regular, al menos una vez por semana, para detectar y eliminar posibles amenazas.

9. Respuesta a Incidentes de Seguridad

- **Reporte Inmediato:** Cualquier incidente de seguridad, como la pérdida de un dispositivo, el acceso no autorizado a un sistema o un ataque cibernético, debe ser reportado de inmediato al Departamento de Informática y a la jefatura directa.
- **Procedimiento de Respuesta:** El Hospital de Iquique cuenta con un procedimiento de respuesta a incidentes de seguridad que detalla los pasos a seguir en caso de un incidente. Todo el personal debe conocer este procedimiento y estar preparado para colaborar en su implementación.
- **Preservación de Evidencia:** En caso de un incidente de seguridad, es importante preservar cualquier evidencia relevante, como registros de acceso, archivos o correos electrónicos, para facilitar la investigación.

10. Capacitación y Concientización

El Hospital de Iquique proporcionará capacitación y concientización periódica sobre ciberseguridad a todo el personal. Esta capacitación cubrirá temas como:

- La importancia de la ciberseguridad en el entorno hospitalario.
- Las pautas y obligaciones establecidas en este instructivo.
- Cómo identificar y prevenir amenazas de ciberseguridad comunes, como el phishing, el malware y los ataques de ingeniería social.
- Cómo reportar incidentes de seguridad.
- Las consecuencias del incumplimiento de las políticas de ciberseguridad.

11. Revisión y Actualización

Este instructivo será revisado y actualizado periódicamente por el Comité de Ciberseguridad del Hospital de Iquique para garantizar que refleje las últimas amenazas de ciberseguridad y las mejores prácticas en la materia. Se notificará a todo el personal sobre cualquier cambio o actualización.

12. Cumplimiento

El incumplimiento de este instructivo puede dar lugar a medidas disciplinarias, de acuerdo con las políticas y procedimientos del hospital.

13. Notificaciones

Se establece que cualquier funcionario que presencie acciones que contravengan el presente instructivo de ciberseguridad tiene la obligación de comunicarlo a su superior jerárquico inmediato. Asimismo, se asigna a los Jefe(a) de Servicios, Jefe(a) de Unidades. Supervisor(a), Coordinador(a) la responsabilidad de notificar al comité de ciberseguridad cualquier acto expuesto o presenciado, en concordancia con lo estipulado en el presente documento.

14. Consideraciones

Este instructivo ha sido elaborado considerando las disposiciones de la legislación vigente en Chile, incluyendo:

- Ley N° 19.628, sobre protección de datos de carácter personal, en lo que respecta al tratamiento de datos sensibles.
- Ley N° 20.584, que regula los derechos y deberes de los pacientes.
- Ley N° 21.113, sobre ciberseguridad.

15.- Glosario

Glosario de Términos de Ciberseguridad - Hospital de Iquique

Actividad Sospechosa o Maliciosa: Cualquier correo electrónico, mensaje o acción que parezca inusual, potencialmente dañina o diseñada para comprometer la seguridad de los sistemas o la información.

Amenazas (Ciberseguridad): Cualquier circunstancia o evento con el potencial de dañar los sistemas informáticos, las redes o la información. Ejemplos incluyen phishing y malware.

Contraseña: Código secreto utilizado para verificar la identidad de un usuario y permitir el acceso a sistemas o información.

Credenciales: Conjunto de información (generalmente un nombre de usuario y una contraseña) utilizada para autenticar y autorizar el acceso a un sistema o recurso.

Ciberseguridad: Prácticas y tecnologías diseñadas para proteger los sistemas informáticos, las redes y la información digital de accesos no autorizados, daños o ataques.

Datos Móviles Personales: La conexión a internet a través del plan de datos de un dispositivo móvil personal (teléfono, tablet u otro dispositivo personal con conexión a Internet).

Departamento de Informática: La unidad o sección responsable de la gestión, mantenimiento y seguridad de los sistemas informáticos del hospital.

Dispositivos de Almacenamiento Externo: Hardware utilizado para guardar datos fuera del equipo principal, como unidades flash USB o discos duros externos.

Divulgación No Autorizada: La acción de revelar información confidencial a personas que no tienen permiso para acceder a ella.

Equipo Computacional: Dispositivo electrónico utilizado para procesar datos, como computadoras de escritorio, laptops, otro dispositivo personal con conexión a Internet).

Equipos Clínicos: Dispositivos informáticos o electrónicos utilizados directamente en la atención y diagnóstico de pacientes.

Escritorio limpio (ciberseguridad): Es la práctica de mantener la superficie de trabajo física y el entorno digital del computador libres de cualquier información sensible o confidencial cuando el usuario no está presente. Esto incluye documentos impresos, notas, dispositivos USB y archivos o aplicaciones con datos importantes visibles en la pantalla.

Hardware: Los componentes físicos de un sistema informático (ej. PC, mouse, teclado, pantalla).

Incidente de Seguridad: Cualquier evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información o los sistemas de información.

Información Estratégica: Datos críticos para la operación y el éxito del hospital, cuya pérdida o divulgación podría tener consecuencias significativas.

Información Clínica: Datos relacionados con la salud y la atención de los pacientes.

Integridad de los Datos: La garantía de que la información es precisa, completa y no ha sido alterada sin autorización.

Jefatura Directa: El superior inmediato de un empleado dentro de la estructura organizacional del hospital.

Malware: Software malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el consentimiento del propietario (ej. virus, troyanos).

Memoria Flash: Tipo de almacenamiento de datos no volátil que puede borrarse y reprogramarse eléctricamente. Funciona sin piezas móviles, lo que la hace duradera y rápida, ideal para dispositivos como pendrives, SSDs, tarjetas de memoria y smartphones.

Notificación: La acción de informar o comunicar formalmente sobre un evento o situación relevante.

Periféricos: Dispositivos externos que se conectan a una computadora (ej. mouse, teclado, pantalla).

Phishing: Un tipo de fraude en línea donde se intenta engañar a las personas para que revelen información confidencial (ej. contraseñas, datos bancarios) haciéndose pasar por entidades legítimas a través de correos electrónicos, mensajes, etc.

Procedimiento de Respuesta a Incidentes: Un conjunto de pasos definidos que se deben seguir al ocurrir un incidente de seguridad.

Protocolos de Respuesta a Incidentes: Las directrices y acciones específicas que se activan en caso de un incidente de seguridad.

Red Informática: El conjunto de equipos informáticos y dispositivos interconectados que permiten compartir recursos e información dentro del hospital.

Riesgo de Daños: La probabilidad de que ocurran eventos que puedan afectar negativamente los sistemas o la información.

Router o Enrutador: Dispositivo que distribuye el flujo de paquetes de información entre redes de la manera más eficaz.

Seguridad de la Red: Las medidas implementadas para proteger la red informática contra accesos no autorizados, ataques o interrupciones.

Señal de Internet Privada: La conexión a internet proporcionada por un dispositivo personal (router, teléfono móvil) en contraposición a la red institucional del hospital.

Software: Los programas informáticos que se ejecutan en un sistema.

Software Antivirus: Un tipo de software diseñado para prevenir, detectar y eliminar malware.

Software No Autorizado: Programas o aplicaciones que no han sido aprobados por el Departamento de Informática para su uso en los sistemas del hospital.

Software de VPN (Red Privada Virtual): Un software que crea una conexión de red segura y cifrada a través de una red pública, pudiendo en algunos casos saltar las reglas de seguridad establecidas.

Sustracción de Información: La copia o el robo no autorizado de datos.

Sistemas Institucionales: Los programas, plataformas y redes informáticas propiedad del Hospital de Iquique y utilizados para sus operaciones.

Trazabilidad: La capacidad de rastrear y registrar las acciones realizadas en los sistemas informáticos, identificando al usuario responsable.

Túneles Informáticos: Un método para crear una conexión segura a través de una red menos segura, similar a una VPN.

Uso Adecuado: La utilización de los recursos informáticos de acuerdo con las políticas y normativas establecidas por la institución.

16. Vía de Comunicación

Le solicitamos utilizar este canal para cualquier notificación de incidentes, solicitudes de información, o cualquier otra comunicación relacionada con CIBERSEGURIDAD o SEGURIDAD DE LA INFORMACIÓN o área relevante al comité.

- Mail: **comiteciberseguridad_hetg@minsal.cl**
- Sr. Eric Ossandon Miranda – Jefe TIC HDI
  Anexo Minsal 575858 – Fono 57-2405858
- Sr. Gerardo Gemio Andia – Administrador de Sistemas Radiológicos HDI
  Anexo Minsal 576584 - Fono 57-2406584

17. Firmas integrantes Comité de Ciberseguridad año 2025, Hospital Dr. Ernesto Torres Galdames. Resolución Exenta N°1763 del 08.08.2024.-

Dr. Aldo Cañete Soto
Director Hospital

Marcela Wachtendorff Valencia
Jefe Departamento Jurídico

Cristian Rojas Pacheco
Jefe Unidad de Grupo Relacionado a Diagnóstico

Cristian Palacios Reyes
Subdirector Administrativo(S)

Fresia Amas Vilca
Jefe Unidad de Planificación y Control de Gestión Hospitalaria

Juan Carlos Vega Damke
Subdirector de Gestión y Desarrollo de las Personas

Mauricio Chandía Nuñez
Jefe Unidad de Estadística y Gestión de la Información en Salud

Eric Ossandon Miranda
Encargado de Seguridad y ciberseguridad de la Información.

Gerardo Gemio Andia
Funcionario Encargado de RISPAC

COMITÉ DE CIBERSEGURIDAD
Y SEGURIDAD DE LA INFORMACIÓN
HOSPITAL DE IQUIQUE
DR. ERNESTO TORRES GALDAMES