Asesoría jurídica

Mat.: Aprueba *"Plan de Recuperación de desastres TI"*.

Santiago.

VISTOS, Lo dispuesto en:

1. El Decreto con Fuerza de Ley N° 1, de 2005, del Ministerio de Salud, que fija texto refundido, coordinado y sistematizado del Decreto Ley N°2.763, de 1979, y de las leyes N^{os}. 18.933 y 18.469;

2. El Decreto con Fuerza de Ley N° 1/19.653, de 2001, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado;

3. La Ley N°19.880, sobre Bases de los Procedimientos Administrativos de los Órganos del Estado;

4. Los Decretos Supremos N° 140/2004 y N° 38/2005, ambos del Ministerio de Salud, que aprueban los reglamentos orgánicos de los Servicios de Salud y de los Establecimientos de Autogestión en Red;

5. La Resolución N° 36/2024, de la Contraloría General de la República, que establece los actos administrativos exentos del trámite de toma de razón.

6. La Resolución Exenta RA N°116675/92/2024, de 30 de enero de 2024, que modifica la Resolución Exenta RA N°116675/419/2023, del Servicio de Salud Metropolitano Central, que nombra en calidad de titular el cargo de Director del Hospital de Urgencia Asistencia Pública.

XASV

CONSIDERANDO

a) Que, el Hospital de Urgencia Asistencia Pública, como establecimiento autogestionado de alta complejidad del Servicio de Salud Metropolitano Central, depende de manera crítica de sus sistemas de información y de la infraestructura tecnológica asociada para garantizar la continuidad de la atención clínica, la seguridad del paciente y el funcionamiento regular de los procesos administrativos y de apoyo.

b) Que, la creciente digitalización de los procesos hospitalarios, junto con el aumento sostenido de incidentes tecnológicos y de ciberseguridad a nivel nacional e internacional, constituye un riesgo relevante para la disponibilidad, integridad y confidencialidad de la información institucional, pudiendo afectar directamente la oportunidad y calidad de la atención en un hospital de urgencia.

c) Que, el presente Plan de Recuperación de Desastres de Tecnologías de la Información tiene por objeto establecer un marco formal, sistemático y trazable para la recuperación oportuna de los sistemas de información y de la infraestructura tecnológica crítica del HUAP frente a incidentes mayores, desastres naturales o eventos tecnológicos, definiendo tiempos objetivos de recuperación (RTO), puntos de recuperación de datos (RPO) y estrategias de continuidad operativa.

d) Que, este instrumento define roles, responsabilidades, flujos de comunicación y procedimientos técnicos para la activación, ejecución, seguimiento y cierre del plan, articulando la labor de la Unidad de Tecnologías de la Información, el Encargado de Ciberseguridad, las jefaturas institucionales, las unidades clínicas y los proveedores críticos, en concordancia con las directrices del Ministerio de Salud y los estándares internacionales de seguridad de la información, tales como la norma ISO/IEC 27002:2022.

e) Que, de conformidad con lo anterior, en el ejercicio de lo dispuesto en el artículo 23 letra c) del Decreto Supremo N°38. De 2005, del Ministerio de Salud, que contiene el Reglamento Orgánico de los Establecimientos de Salud de Menor Complejidad y de los Establecimientos de Autogestión en Red, según el cual le corresponde al Director organizar internamente el Establecimiento Autogestionado y

f) asignar las tareas correspondientes, con el fin de atender las necesidades públicas o colectivas de una manera regular, continua y permanente, como lo ordenan los artículos 3° y 28 de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, y con la finalidad de establecer la ***primera versión*** del *"Plan de Recuperación de desastres TI"*, dicto la siguiente:

RESOLUCIÓN

I. APRUÉBANSE la ***primera versión*** del *"Plan de Recuperación de desastres TI"*, que es del siguiente tenor:

Servicio de Salud Metropolitano Central – Ministerio de Salud	PLAN RECUPERACION DE DESASTRES TI				
	CÓDIGO UTIC	VERSIÓN 01	FECHA 12/2025	VIGENCIA 5 años	N° PÁGINAS 21

HOSPITAL DE URGENCIA ASISTENCIA PUBLICA

Revisado Por:	Aprobado Por:
Firmado por: Karla Andrea Alfaro Flores, Jefatura Calidad y Seguridad del Paciente, Fecha: 26-12-2025 11:23 CLT, Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río	Firmado por: Jorge Arturo Ibáñez Parga, Director Huap (s), Fecha: 29-12-2025 19:29 CLT, Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/D1HF2N-699

ÍNDICE:

I. INTRODUCCIÓN 3
II. OBJETIVOS 4
III. ALCANCE 5
IV. DEFINICIONES 5
V. RESPONSABLES DE LA EJECUCIÓN 6
VI. DESARROLLO DEL PROCESO 7
VII. CONTINGENCIAS 12
VIII. REVISION 13
IX. DISTRIBUCIÓN 14
X. REFERENCIAS BIBLIOGRÁFICAS 14
XI. MODIFICACIONES DEL DOCUMENTO 15
XI. ANEXOS 16

I. INTRODUCCIÓN

El Hospital de Urgencia Asistencia Pública (HUAP), como establecimiento de alta complejidad del Servicio de Salud Metropolitano Central, depende en forma crítica de sus sistemas de información y de la infraestructura tecnológica asociada (servidores, redes, almacenamiento y enlaces de comunicaciones). Estos sistemas sustentan tanto la atención clínica de pacientes como los procesos administrativos y de apoyo, por lo que su interrupción representa un riesgo significativo para la continuidad asistencial y la seguridad del paciente.

A nivel nacional, la Estrategia de Ciberseguridad en Salud 2023–2030 del Ministerio de Salud señala que los incidentes de ciberseguridad en hospitales se han incrementado en más de un 60% en los últimos cinco años, siendo los ataques de ransomware y las fallas de infraestructura tecnológica los eventos más reportados. Estudios internacionales muestran que la caída de sistemas clínicos críticos puede retrasar la atención de urgencia hasta en un 30%, aumentando el riesgo de eventos adversos y mortalidad prevenible (WHO, 2022).

En este contexto epidemiológico y tecnológico, se hace necesario contar con un Plan de Recuperación de Desastres de Tecnologías de la Información (PRD TI) que permita:

- Restablecer oportunamente los sistemas y servicios críticos en los tiempos definidos (RTO) y con la mínima pérdida de información (RPO).
- Asegurar la continuidad de la atención clínica y administrativa, reduciendo el impacto de contingencias mayores.
- Cumplir con las directrices del Ministerio de Salud de Chile en materia de ciberseguridad y continuidad operativa, en concordancia con el control ISO/IEC 27002:2022, 5.29 – Seguridad de la Información durante la Interrupción.

La aplicación de este protocolo abarca no solo los sistemas de información digitales, sino también la plataforma tecnológica completa del HUAP, incluyendo servidores físicos y virtuales, equipos de red, sistemas de respaldo y enlaces de

comunicaciones institucionales. La gestión de la infraestructura de datacenter y su recuperación se realizará en coordinación con el Servicio de Salud Metropolitano Central (SSMC) y proveedores críticos asociados.

Este protocolo está dirigido a la Dirección y Subdirecciones del HUAP, la Unidad de Tecnologías de la Información, las unidades clínicas y que dependen de los servicios tecnológicos, y a los proveedores críticos externos responsables de garantizar la continuidad operativa.

II. OBJETIVOS

General:

Establecer un Plan de Recuperación de Desastres de Tecnologías de la Información (PRD TI) en el Hospital de Urgencia Asistencia Pública (HUAP), con el fin de garantizar la continuidad de los servicios clínicos y administrativos mediante la recuperación oportuna de los sistemas de información y la infraestructura tecnológica crítica frente a incidentes mayores, desastres naturales o tecnológicos.

Específicos:

- Definir procedimientos estandarizados para la activación, ejecución y cierre del PRD TI, considerando sistemas de información, hardware, redes, almacenamiento, datacenter y enlaces de comunicación.

- Asegurar la coordinación entre el personal interno y los proveedores críticos mediante roles definidos, comunicación efectiva y pruebas periódicas de recuperación, en concordancia con las directrices del MINSAL y la norma ISO/IEC 27002:2022 (5.29).

III. ALCANCE

El presente Plan de Recuperación de Desastres de Tecnologías de la Información (PRD TI) está dirigido a las/los funcionarios del Hospital de Urgencia Asistencia Pública (HUAP) que participan directa o indirectamente en la gestión, operación y uso de los sistemas de información y de la plataforma tecnológica institucional.

IV. DEFINICIONES

- **HUAP:** Hospital de Urgencia Asistencia Pública.
- **SSMC:** Servicio de Salud Metropolitano Central.
- **MINSAL:** Ministerio de Salud de Chile.
- **Activo crítico de TI:** Cualquier sistema, servicio, hardware, red o dato cuya interrupción afecta la continuidad de la atención clínica o administrativa del HUAP.
- **Plataforma tecnológica:** Conjunto de sistemas de información, servidores, almacenamiento, redes, datacenter y enlaces de comunicaciones bajo responsabilidad del hospital.
- **Sistema de información crítico:** Aplicación o servicio tecnológico esencial para la operación clínica o administrativa (ej.: SINA, Active Directory, correo institucional).
- **Datacenter:** Instalación física que alberga servidores, redes, sistemas de respaldo y servicios de misión crítica.
- **RTO (Recovery Time Objective):** Tiempo máximo aceptable para restaurar un sistema o servicio tras una contingencia.
- **RPO (Recovery Point Objective):** Cantidad máxima de datos que puede perderse medida en tiempo (ej.: 24 horas).
- **Incidente mayor / desastre tecnológico:** Evento que afecta la disponibilidad de sistemas críticos por más de 60 minutos, compromete información sensible o requiere restauración desde respaldos.
- **Respaldo (Backup)**: Copia de seguridad de datos críticos destinada a permitir su recuperación en caso de pérdida, corrupción o incidente.

- **Proveedor crítico:** Entidad externa con contrato vigente que da soporte a la operación de sistemas o infraestructura esencial (ej.: Entel, SSMC).

V. RESPONSABLES DE LA EJECUCIÓN

Responsable de Ejecución

- **Encargado/a de Ciberseguridad y Seguridad de la Información:** valida respaldos, verifica la integridad de los datos, controla accesos durante la recuperación y documenta incidentes, tiempos y resultados.

- **Encargado/a de Infraestructura TI:** evalúa la magnitud del incidente, activa a los proveedores de soporte y supervisa la restauración de servidores, red y datacenter.

- **Equipo de Soporte Técnico (Nivel 1 y 2):** ejecuta tareas operativas de recuperación (diagnóstico, restauración, soporte a usuarios) y reporta avances a la Jefatura TIC.

- **Proveedores críticos externos (Entel, SSMC, otros):** brindan soporte especializado según contrato y acuerdos de nivel de servicio (SLA), participando en la restauración de infraestructura y comunicaciones externas.

Responsable de Supervisión

- **Jefatura de Unidad de Tecnología de la Información (TIC):** coordina la activación del PRD TI, lidera la continuidad de servicios tecnológicos, supervisa la ejecución de las acciones de recuperación e informa a la Dirección del HUAP sobre el estado del plan.

VI. DESARROLLO DEL PROCESO

Inicio del Protocolo

El presente protocolo se activa frente a un incidente mayor o desastre tecnológico que afecte la continuidad de los servicios clínicos o administrativos del Hospital de Urgencia Asistencia Pública de acuerdo con los criterios definidos en el **Anexo N°5 – Clasificación de Desastres,** disponible en la carpeta institucional de la Unidad de Tecnologías de la Información**.**

Desarrollo del Proceso

El proceso de Recuperación de Desastres TI contempla las siguientes fases:

1. **Detección y notificación del incidente:**

- La **Mesa de Ayuda (24/7)** recibe, registra y gestiona los reportes de incidentes a través de ticket, teléfono o correo institucional.

- **Clasificación del incidente**: La Mesa de Ayuda debe clasificar el incidente dentro de los siguientes plazos:

    - Incidente crítico: máximo **30 minutos.**
    - Incidente de media o baja criticidad: máximo **60 minutos.**

- **Incidente normal vs. posible desastre:**
    - Si se trata de un **incidente de soporte TI**, entendido como una falla tecnológica de baja o media criticidad que no afecta sistemas críticos ni la continuidad asistencial, se gestiona conforme a los procedimientos habituales de soporte de la Unidad de Tecnologías de la Información.
    - Si el incidente cumple criterios de **posible desastre**, la Mesa de Ayuda debe **escalar inmediatamente** la situación a los responsables TIC definidos en el presente protocolo.

2. **Evaluación inicial del impacto:**

- La Mesa de Ayuda, en conjunto con los responsables TIC, realiza una evaluación inicial del impacto del incidente considerando:
    - Usuarios y unidades afectadas.
    - Inventario de activos críticos (Anexo N°1).
    - Clasificación de Desastres (Anexo N°5).
- El incidente será considerado **desastre tecnológico** si se cumple al menos uno de los siguientes criterios:
    - Supera los tiempos máximos de recuperación (RTO) definidos en el Anexo N°5.
    - Afecta sistemas de información críticos.
    - Compromete datos sensibles o la privacidad de pacientes o funcionarios.
    - Requiere la participación de proveedores externos o soporte especializado (Anexo N°2).
    - Compromete la operación del hospital de forma prolongada o extensa (más de 24 horas).

3. **Declaración de emergencia y activación del PRD:**

- **En horario hábil:** La **activación formal del Plan de Recuperación de Desastres TI** podrá ser realizada por la **Jefatura TIC**, el/la **Encargado/a de Ciberseguridad y Seguridad de la Información** o el/la **Encargado/a de Infraestructura TI**, idealmente con la validación de al menos dos de estos responsables.

- **En horario inhábil:** La **Mesa de Ayuda** tiene la responsabilidad de **detectar, registrar, clasificar y escalar** inmediatamente los incidentes que cumplan criterios de desastre**.**

En caso de no lograr contacto con ninguno de los responsables definidos en un plazo máximo de **30 minutos**, la Mesa de Ayuda podrá **activar el protocolo en carácter excepcional y preventivo**, dejando registro formal de la decisión y notificando a la Jefatura TIC a la brevedad.

- **Notificación:** La activación del PRD TI será comunicada a la Dirección del HUAP, a los proveedores críticos (Anexo N°3) y a las unidades afectadas, **dentro de un plazo máximo de 30 minutos desde su activación**, a través de los canales oficiales de contacto (correo institucional y/o teléfono directo).

4. **Ejecución de estrategias de recuperación**

- Los servicios afectados serán restaurados conforme a los procedimientos y prioridades definidos en el **Anexo N°5 – Clasificación de Desastres (Tabla Operativa)**, **documento de uso interno y acceso restringido de la Unidad de Tecnologías de la Información**, disponible en el **repositorio institucional de Informática**, priorizando la recuperación según la criticidad del activo.

- **Validación de servicios restaurados:** Cada servicio restaurado debe ser validado **técnicamente por la Unidad de Tecnologías de la Información** y **funcionalmente por los usuarios responsables o referentes de la unidad afectada**, antes de ser habilitado nuevamente para su uso productivo.

- **Soporte externo:** Si la recuperación excede las capacidades internas, se activa soporte externo según los SLA acordados con proveedores (Anexo 2).

5. **Comunicación durante la recuperación:**

- **Mesa de Ayuda:** informa a los usuarios afectados sobre el estado de la recuperación **con una frecuencia mínima cada 2 horas**, o antes, en caso de producirse cambios relevantes en el estado del incidente o en los tiempos estimados de recuperación.
- **Equipo TIC:** reporta a la Dirección del HUAP y a los responsables definidos **dentro de las primeras 2 horas desde la activación del PRD TI**, y posteriormente **con una frecuencia mínima cada 4 horas**, manteniendo trazabilidad de las acciones realizadas.

- **Comunicación interna:** aviso a la Dirección del HUAP, Subdirecciones correspondientes y responsables de sistemas afectados **dentro de la primera hora desde la activación del PRD TI**.

- **Comunicación a usuarios:** informar al personal clínico y administrativo sobre la afectación y los tiempos estimados de recuperación **dentro de las primeras 2 horas desde la activación del PRD TI**, y luego conforme a las actualizaciones entregadas por la Mesa de Ayuda.

- **Comunicación con proveedores:** contacto con proveedores críticos (SSMC, Entel, SINA, entre otros) **dentro de la primera hora desde la activación del PRD TI**, o antes si la naturaleza del incidente lo requiere.

- **Comunicación externa:** se realizará exclusivamente a través de la Dirección del HUAP y la Unidad de Comunicaciones, **una vez confirmada la magnitud del incidente**, en caso de que corresponda informar a MINSAL, medios u otros actores externos.

- **Registro de comunicaciones:** toda comunicación debe quedar documentada y archivada como parte de la evidencia del incidente (Anexo N°4), **durante todo el período de activación del PRD TI** y hasta el cierre formal del incidente, en una carpeta de contingencias definida y administrada por la Unidad TIC, ya sea en formato digital (servidor institucional o sistema de Mesa de Ayuda) o físico, según lo que determine la propia unidad.

6. Cierre y documentación del incidente:

- **Informe Post-Incidente:** El/la Encargado/a de Ciberseguridad y Seguridad de la Información elabora un informe detallado del incidente, **el cual deberá ser entregado a la Jefatura de la Unidad de Tecnologías de la Información y a la Dirección del HUAP dentro de un plazo máximo de 5 días hábiles desde el cierre del incidente**, e incluirá:

  - Servicios afectados.
  - Acciones realizadas.
  - Tiempos RTO/RPO logrados.
  - Lecciones aprendidas (Anexo 4).

- **Validación de servicios restaurados:** La recuperación debe ser validada en dos etapas:

  - **Validación técnica:** realizada por el Equipo TIC, confirmando conectividad, accesos y registros sin errores.

  - **Validación funcional**: realizada por usuarios clave de cada sistema afectado, verificando que las aplicaciones y procesos clínicos/administrativos funcionen normalmente.

- **Validación y presentación:** La Jefatura TIC valida el informe y lo presenta al Comité de Ciberseguridad.

- **Archivado de la documentación:** La documentación relacionada con el incidente se conserva por un período mínimo de tres años para futuras auditorías o revisiones, en una carpeta de contingencias definida y administrada por la Unidad TIC (repositorio digital institucional o archivo físico, según lo determine la unidad).

Término del Protocolo

El protocolo se considera concluido con la elaboración, validación y difusión del Informe Post-Incidente a la Dirección HUAP, Subdirecciones, Comité de Ciberseguridad y Unidades Clínicas y Administrativas afectadas.

En caso de contingencias que hayan generado impacto clínico, asistencial o legal, el informe deberá ser difundido además a las unidades correspondientes, tales como **Calidad, IAAS, Jurídica u otras que determine la Dirección del HUAP**, según la naturaleza del incidente.

VII. CONTINGENCIAS

Se consideran contingencias aquellas situaciones de emergencia que pueden interrumpir o dificultar la correcta implementación del presente Plan de Recuperación de Desastres TI en el Hospital de Urgencia Asistencia Pública (HUAP).

Entre ellas se incluyen:

- Fallas tecnológicas críticas que imposibiliten la ejecución de las fases del protocolo (ejemplo: caída total de servidores, corrupción de bases de datos, daño en equipos de red).

- Interrupciones de infraestructura que afecten la disponibilidad del datacenter o salas de servidores (cortes prolongados de energía, fallas de climatización, incendio o inundación).

- Contingencias de comunicaciones que impidan el enlace con usuarios o proveedores (corte de Internet institucional o fallas en enlaces redundantes).

- Incidentes de ciberseguridad de alto impacto (ataques de ransomware, DDoS o accesos no autorizados que impidan operar los sistemas).

- Eventos externos de gran magnitud como sismos, incendios, inundaciones o emergencias sanitarias que restrinjan el acceso a las instalaciones o limiten el despliegue del personal TIC.

En todos estos casos, la activación del protocolo y la definición de medidas alternativas será responsabilidad de la Jefatura de Tecnologías de la Información o del Encargado/a de Ciberseguridad y Seguridad de la Información, quienes deberán asegurar la continuidad operativa mediante acciones de recuperación parcial o total de los sistemas afectados.

VIII. REVISION

El presente Plan de Recuperación de Desastres TI será revisado y actualizado conforme a los siguientes lineamientos:

- **Periodicidad:** revisión formal anual, liderada por la Jefatura TIC en coordinación con el/la Encargado/a de Ciberseguridad.

- **Actualización anticipada**: se deberá revisar y actualizar el protocolo en caso de:
  - Cambios relevantes en la infraestructura tecnológica.
  - Modificación de proveedores críticos o servicios tercerizados.
  - Incorporación o reemplazo de sistemas de información críticos.
  - Cambios en responsables o estructura organizacional de la UTIC.

- **Control de Cambios:** toda actualización será registrada en la tabla de Modificaciones del Documento.

- **Pruebas de validación:** al menos una vez al año se deberá realizar un ejercicio de recuperación parcial o total, documentando resultados y corrigiendo brechas detectadas.

Responsable de la revisión: Jefatura de la Unidad de Tecnologías de la Información, con apoyo del/la Encargado/a de Ciberseguridad y Seguridad de la Información.

IX. DISTRIBUCIÓN

1. Dirección
2. Subdirección de Gestión Administrativa y Financiera
3. Subdirección de Gestión del Cuidado.
4. Subdirección de Gestión y Desarrollo de las Personas.
5. Subdirección de Gestión Clínica
6. Unidad de Calidad y Seguridad del Paciente
7. Unidad de Tecnología de la Información

X. REFERENCIAS BIBLIOGRÁFICAS

- International Organization for Standardization. (2022). *ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls*. Ginebra, Suiza: ISO.
- Ministerio de Salud de Chile. Subsecretaría de Redes Asistenciales. (2023). *Estrategia Nacional de Ciberseguridad en Salud 2023–2030*. Santiago, Chile: MINSAL.
- Ministerio de Salud de Chile. División de Gestión de la Red Asistencial. (2025). *Orientaciones técnicas COMGES 2025 – Indicador de Ciberseguridad*. Santiago, Chile: MINSAL.

XI. MODIFICACIONES DEL DOCUMENTO

SÍNTESIS DE MODIFICACIONES			RESPONSABLE MODIFICACIÓN	APROBADO POR
VERSIÓN	FECHA	CAUSA DE MODIFICACIÓN		
01	12/2025	Creación del Documento	Enzo Mayo G. Encargado Ciberseguridad	Dr. Patricio Barría

XI. ANEXOS

ANEXO N° 1: Inventario de Activos Críticos TIC:

- El Inventario de Activos Críticos TIC del Hospital de Urgencia Asistencia Pública (HUAP) corresponde a una **tabla de uso interno**, que contiene información sensible sobre infraestructura, sistemas y servicios tecnológicos críticos.

  Por razones de seguridad de la información, dicho inventario **no se incorpora íntegramente en el presente protocolo**.

  El documento se encuentra disponible y actualizado en el **repositorio institucional de la Unidad de Tecnologías de la Información**, con acceso restringido al personal autorizado

INVENTARIO DE ACTIVOS

N°	Nombre del Activo	Tipo	Descripción	Responsable	URL	Ubicación	Confidencialidad	Disponibilidad	Integridad	Criticidad	Crítico CO
1	Computadores (Estaciones de trabajo, Laptops, PC de escritorio)	Hardware	Dispositivos para tareas operativas y administrativas del hospital	Equipo de Soporte	No aplica	Diferentes áreas del hospital	Medio	Alto	Medio	Alto	Medio
2	Teléfonos IP	Hardware	Teléfonos utilizados para la comunicación interna y externa autorizados por el hospital	Equipo de Soporte	No aplica	Diversas dependencias del hospital	Bajo	Medio	Bajo	Bajo	Bajo
3	Impresoras y Equipos Multifuncionales	Hardware	Dispositivos para impresión, escaneo y fotocopias	Dimacofi	No aplica	Distintas oficinas del hospital	Medio	Medio	Bajo	Medio	Bajo
4	Servidores	Hardware / Software	Equipos que alojan aplicaciones, bases de datos y sistemas hospitalarios	Infraestructura TI	No aplica	Data center / Cloud	Alto	Alto	Alto	Alto	Alto
5	UPS (Uninterruptible Power Supply)	Hardware	Dispositivos para asegurar continuidad en caso de fallos eléctricos	Equipo de Soporte	No aplica	N/A	Bajo	Alto	Bajo	Alto	Alto (revisar)
6	Dispositivos de almacenamiento externo (Discos duros, USB, etc.)	Hardware	Almacenamiento de información sensible y respaldos	Equipo de Soporte	No aplica	N/A	Alto	Medio	Alto	Alto	Alto (revisar)
7	Sistemas de gestión clínica y departamental (SINA, Florence, HIS)	Software	Sistemas de gestión clínica y administrativa (Rayen Salud)	TIC	Cliente-servidor	Infraestructura local	Alto	Alto	Alto	Alto	Alto
8	Plataforma de correo electrónico	Software	Correo electrónico para comunicación interna y externa	Infraestructura TI	Acceso vía navegador / App	Cloud	Medio	Medio	Medio	Medio	Medio
9	Navicat	Software	Cliente de gestión y conexión a bases de datos	Infraestructura TI	Aplicación local	Máquina virtual	Alto	Alto	Alto	Alto	Medio
10	VPN	Software	Red privada virtual para acceso remoto seguro	SSMC	Cliente VPN	Cloud + Servidores locales	Alto	Medio	Alto	Alto	Medio (revisar)
11	Infraestructura de Red Local	Redes de comunicación	Equipos que gestionan conectividad y tráfico de datos	Entel	No aplica	Dependencias del hospital	Medio	Alto	Medio	Alto	Alto
12	Innhosp – Aplicación Web	Software	Gestión de personal a contrata y honorarios, control de marcaciones	Infraestructura TI / Desarrollo TIC	https://innhosp.huap.online	Oracle Cloud (pronto local)	Alto	Alto	Alto	Alto	Medio
13	Jefatura – Aplicación Web	Software	Submódulo de Innhosp para gestión de jefaturas	Infraestructura TI / Desarrollo TIC	https://jefatura.huap.online	Oracle Cloud (pronto local)	Alto	Alto	Alto	Alto	Medio
14	Personal – Aplicación Web	Software	Submódulo de Innhosp para colaboradores	Infraestructura TI / Desarrollo TIC	https://personal.huap.online	Oracle Cloud (pronto local)	Alto	Alto	Alto	Alto	Medio
15	Aplicación de Gestión de Nutrición – Aplicación Web	Software	Gestión de visitas clínicas y regímenes alimenticios	Infraestructura TI / Desarrollo TIC	https://nutricion.huap.local	Infraestructura local	Alto	Alto	Alto	Alto	Medio
16	ERP-Free – Aplicación Web	Software	Sistema de gestión de insumos y bodegas	Infraestructura TI / Desarrollo TIC	http://10.6.15.33:8589	Infraestructura local	Medio	Medio	Medio	Medio	Medio
17	Módulo de Control de Marcaciones	Software	Registro de entradas y salidas con huella/clave	Infraestructura TI / Desarrollo TIC	App instalada en PCs	IPs específicas HUAP	Alto	Alto	Alto	Alto	Bajo
18	Módulo de Control de Acceso a Casino	Software	Registro de acceso a casino con huella/clave	Infraestructura TI / Desarrollo TIC	App instalada en PCs	IPs específicas HUAP	Alto	Alto	Alto	Alto	Bajo
19	Documentos – Aplicación Web	Software	Almacenamiento de documentos digitalizados de Calidad	Infraestructura TI / Desarrollo TIC	https://documentos.huap.online	Oracle Cloud (pronto local)	Alto	Alto	Alto	Alto	Bajo
20	Documentos laboratorio – Aplicación Web	Software	Almacenamiento de documentos digitalizados de laboratorio	Infraestructura TI / Desarrollo TIC	https://laboratorio.huap.online	Oracle Cloud (pronto local)	Alto	Alto	Alto	Alto	Bajo
21	Módulo de Enrolamiento de Huellas	Software	Registro de huellas de colaboradores	Desarrollo TIC	App instalada en PCs	Honorarios / RRHH	Alto	Alto	Alto	Alto	Bajo
22	Carpeta Compartida	Almacen de Datos	Carpeta de red para trabajo colaborativo y respaldos	Infraestructura TI	\\10.6.15.54\Desarrollo	Infraestructura local	Alto	Alto	Alto	Alto	Medio
23	FLORENCE	Software	Ficha clínica electrónica	TIC	Cliente local	Infraestructura local	Alto	Alto	Alto	Alto	Alto

ANEXO N° 2: Identificación de Sites / Datacenters:

- Para efectos de contacto y coordinación para la atención y revisión de contingencias, a continuación, se presentan los datos de contacto de ambas partes, Minsal y Entel.

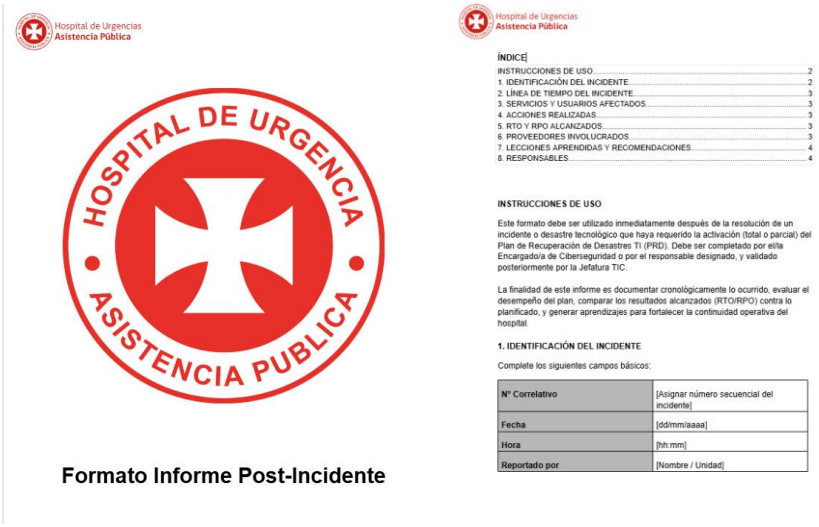
Rol	Responsable	Nombre	Teléfono	Correo
Unidad Infraestructura, Tecnología y Operaciones	Datacenter HUAP Piso -1 Valech Piso 4	Javier Szperka Huerta	281354	javier.szperka@redsalud.gob.cl
Unidad Telecomunicaciones, Ciberseguridad y Transformación Digital	Responsable de enlaces de comunicaciones institucionales y referente con MINSAL y proveedores críticos (ej. Entel)	Fabiola Pavez Stuardo	289227	fabiola.pavez@redsalud.gob.cl

ANEXO N° 3: Contactos de Emergencia:

- Los responsables de contacto involucrados en el proceso de activación del DRP.

Rol	Responsable	Nombre	Teléfono	Correo
Jefe/a de TIC	Continuidad Operacional	Susana Avendaño D.	281354	susana.avendano@redsalud.gob.cl
Encargado/a de Ciberseguridad y seguridad de la información	Ciberseguridad / Seguridad de la Información	Enzo Ignacio Mayo Gonzalez	285266	enzo.mayo@redsalud.gob.cl
Encargado/a de Infraestructura	Infraestructura TI	Alejandro Gonzalez Perez	281138	alejandro.gonzalez.p@redsalud.gob.cl
Jefe/a de Desarrollo	Administración de Desarrollo y Bases de datos	Arturo Moya Gonzalez	281256	arturo.moya@redsalud.gob.cl
Proveedor Externo (Entel, SSMC, etc)	Soporte Externo Enlaces			

ANEXO N° 4: Formato Informe Post-Incidente:



Hospital de Urgencias Asistencia Pública

HOSPITAL DE URGENCIA ASISTENCIA PUBLICA

Formato Informe Post-Incidente

Hospital de Urgencias Asistencia Pública

ÍNDICE

INSTRUCCIONES DE USO 2
1. IDENTIFICACIÓN DEL INCIDENTE 2
2. LÍNEA DE TIEMPO DEL INCIDENTE 3
3. SERVICIOS Y USUARIOS AFECTADOS 3
4. ACCIONES REALIZADAS 3
5. RTO Y RPO ALCANZADOS 3
6. PROVEEDORES INVOLUCRADOS 3
7. LECCIONES APRENDIDAS Y RECOMENDACIONES 4
8. RESPONSABLES 4

INSTRUCCIONES DE USO

Este formato debe ser utilizado inmediatamente después de la resolución de un incidente o desastre tecnológico que haya requerido la activación (total o parcial) del Plan de Recuperación de Desastres TI (PRD). Debe ser completado por el/la Encargado/a de Ciberseguridad o por el responsable designado, y validado posteriormente por la Jefatura TIC.

La finalidad de este informe es documentar cronológicamente lo ocurrido, evaluar el desempeño del plan, comparar los resultados alcanzados (RTO/RPO) contra lo planificado, y generar aprendizajes para fortalecer la continuidad operativa del hospital.

1. IDENTIFICACIÓN DEL INCIDENTE

Complete los siguientes campos básicos:

N° Correlativo	[Asignar número secuencial del incidente]
Fecha	[dd/mm/aaaa]
Hora	[hh:mm]
Reportado por	[Nombre / Unidad]

ANEXO N° 5: Clasificación de Desastres (Tabla Operativa):

Anexo 5 – Clasificación de Desastres (Tabla Operativa)

Activo / Sistema	Criticidad	RTO Máx.	Qué hacer (Acción inmediata)	Contacto Responsable
SINA – Florence	Alto	1-2 h	1. Abrir ticket crítico. 2. Avisar Ciberseguridad y Jefatura TIC. 3. Reiniciar servicio o restaurar desde backup. 4. Si ataque: aislar y contactar CSIRT.	
FLORENCE (Clínico principal)	Alto	1-2 h	Igual que SINA: restaurar desde backup o escalar a proveedor.	
Active Directory (AD)	Alto	2 h	1. Notificar Infraestructura. 2. Verificar disponibilidad de DCs. 3. Si un DC falla → restaurar desde snapshot/backup. 4. Validar sincronización de usuarios/servicios críticos (correo, VPN, apps clínicas). 5. Si todos los DC caen → activar servidor de contingencia y restaurar Sysvol.	
Banco de Sangre	Alto	1-2 h	1. Abrir ticket. 2. Activar plan manual (registro físico). 3. Restaurar DB desde backup o contactar soporte laboratorio.	
RIS / PACS	Alto	2-4 h	1. Notificar Radiología. 2. Revisar almacenamiento DICOM. 3. Restaurar desde backup o activar servidor alterno.	
Telemedicina	Alto	2-4 h	1. Revisar conectividad. 2. Reiniciar servicio. 3. Contactar proveedor si no hay solución. 4. Derivar atención a presencial.	
Infraestructura de Red (LAN/WiFi)	Alto	2-4 h	1. Notificar Infraestructura y Entel. 2. Revisar switches/firewalls. 3. Activar enlaces redundantes.	
Servidores (VMs / físicos)	Alto	2-4 h	1. Ticket. 2. Identificar si es host o VM. 3. Restaurar desde snapshot o mover a servidor de contingencia.	
UPS (energía crítica)	Alto	1-2 h	1. Revisar estado batería. 2. Encender generadores. 3. Contactar proveedor de mantención.	
Dispositivos de almacenamiento (NAS/Discos)	Alto	2-4 h	1. Revisar estado RAID. 2. Restaurar desde backup si hay corrupción. 3. Reemplazar disco dañado.	
LIS (Laboratorio)	Alto	2-4 h	1. Notificar laboratorio. 2. Reiniciar servicios DB. 3. Restaurar backup si falla.	

Sistemas de criticidad MEDIA (RTO 2–8 h)

Activo / Sistema	Criticidad	RTO Máx.	Qué hacer (Acción inmediata)	Contacto Responsable
Plataforma de correo	Medio	4–8 h	1. Revisar servicios Exchange/SMTP. 2. Reiniciar. 3. Escalar a proveedor si no hay servicio.	
VPN	Medio	4–8 h	1. Revisar túneles. 2. Reiniciar concentrador VPN. 3. Contactar proveedor si falla.	
Navicat	Medio	8 h	1. Reinstalar cliente. 2. Restaurar configuración. 3. Escalar a DBA si falla (no hay).	
Innhosp / Jefatura / Personal / REDCAP / ERP-Free / ERP / SIGES / ORDEN / RNI (Apps Web)	Medio	8-12 h	1. Ticket. 2. Revisar logs. 3. Reiniciar servicio. 4. Restaurar DB si es necesario.	
Carpeta Compartida (NAS)	Medio	8–12 h	1. Validar permisos. 2. Restaurar desde backup. 3. Dar acceso alternativo.	

Sistemas de criticidad BAJA (RTO 12–24 h)

Activo / Sistema	Criticidad	RTO Máx.	Qué hacer (Acción inmediata)	Contacto Responsable
Computadores (PC/Laptops)	Medio	12–24 h	1. Reimagen del equipo. 2. Reemplazo temporal si es crítico.	
Teléfonos IP	Bajo	12–24 h	1. Reiniciar central. 2. Redirigir anexos críticos a celulares.	
Impresoras / Multifuncionales	Bajo	24–48 h	1. Reinstalar drivers. 2. Usar impresora alterna.	
Módulos menores (Marcaciones, Casino, Huellas, FLORENCE GESTION, SIGFE, SISDOC, LME, HELP, SIRH, ALCOR, Documentos Web)	Bajo	24–48 h	1. Ticket. 2. Reiniciar servicio. 3. Usar plan manual (registro en papel) hasta recuperación.	

Elaborado por:

1. Enzo Mayo G., Encargado de Ciberseguridad y Seguridad de la Información

Revisado por:

1. Susana Avendaño D., Jefa Unidad de Tecnologías de la Información
2. Christian Echeverría A., Subdirector Administrativo y Financiero
3. TM. Camila Benítez U., Profesional Unidad de Calidad y Seguridad del Paciente

Firmado por:
Camila Andrea Benitez Ugarte
Profesional Unidad Calidad y Seguridad del Paciente
Fecha: 23-12-2025 12:04 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Rio

Firmado por:
Luis Arturo Moya González
Jefatura Tic (s)
Fecha: 23-12-2025 16:46 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Rio

Firmado por:
Christian Irving Echeverría Aburto
Subdirector Gestión Administrativa y Financiera
Fecha: 24-12-2025 18:30 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Rio

II. TÉNGASE PRESENTE la vigencia de este plan a contar de la fecha de la total tramitación de la presente Resolución.

III. ESTABLÉCESE que el señalado *"Plan de Recuperación de desastres TI"*, debe ser el que se tenga en consideración a contar de la fecha de su entrada en vigencia.

IV. DÉJESE SIN EFECTO toda normativa interna que diga relación con la materia de este plan.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

FIRMA ELECTRÓNICA AVANZADA
GOBIERNO DE CHILE

Firmado por:
Patricio Raúl Barría Ailef
Director Huap
Fecha: 09-01-2026 16:25 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Distribución:
1. Dirección.
2. Subdirección de Gestión Administrativa y financiera.
3. Subdirección de Gestión del Cuidado.
4. Subdirección de Gestión y Desarrollo de las Personas.
5. Subdireccion de Gestión Clínica.
6. Unidad de Calidad y Seguridad del Paciente.
7. Unidad de Tecnología de la Información.
8. Asesoría Jurídica.
9. Oficina de Partes.

XASV