



Asesoría jurídica

**Mat.:** Aprueba “*Política de Relación con Proveedores*”.

**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°s. 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 Resoluciones N°36, de 2024, y N°8, de 2025, ambas de la Contraloría General de la República, sobre exención del trámite de toma de razón y demás instrucciones aplicables a la tramitación de actos administrativos.

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.



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/IUWMBI-599>

## **CONSIDERANDO**

**a)** Que, el Hospital de Urgencia Asistencia Pública, como establecimiento autogestionado de alta complejidad y órgano integrante de la Administración del Estado, mantiene relaciones permanentes con proveedores y terceros que participan en la provisión de bienes y servicios esenciales para la continuidad de la atención clínica y el funcionamiento institucional.

**b)** Que, dichas relaciones con proveedores pueden implicar acceso a información institucional, datos personales y sensibles, sistemas informáticos, infraestructura tecnológica o procesos críticos del hospital, lo que hace necesario establecer directrices formales que resguarden la confidencialidad, integridad y disponibilidad de la información.

**c)** Que, la presente Política de Relación con Proveedores tiene por objeto establecer los lineamientos administrativos, técnicos y contractuales que regulan la gestión de la seguridad de la información y la ciberseguridad en la relación con proveedores y terceros, incorporando estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002, así como la normativa nacional vigente en materia de protección de datos y ciberseguridad.

**d)** Que, este instrumento define roles y responsabilidades para las unidades institucionales involucradas en los procesos de contratación, supervisión y control de proveedores, incluyendo la Subdirección Administrativa y Financiera, el Departamento de Abastecimiento, la Unidad de Tecnologías de la Información, el Encargado de Ciberseguridad y la Asesoría Jurídica, estableciendo mecanismos de evaluación de riesgos, monitoreo de cumplimiento, gestión de incidentes y aplicación de medidas correctivas o sanciones contractuales.

**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 3º 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** de la “*Política de Relación con Proveedores*”, dicto la siguiente:

## RESOLUCIÓN

**I. APRUÉBANSE** la **primera versión** de la “*Política de Relación con Proveedores*”, que es del siguiente tenor:

		POLÍTICA DE RELACIÓN CON PROVEEDORES				
CÓDIGO UTIC	VERSIÓN	FECHA 01/2026	VIGENCIA 5 años	Nº PÁGINAS 18		



Revisado Por:	Aprobado Por:
 Firmado por: Ilse Dora del Carmen Silva Robles Infraestructura Calidad y Seguridad del Ambiente Fecha: 14-01-2026 09:56 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río	 Firmado por: Patricio Raúl Barria Allef Director Clínico Fecha: 15-01-2026 11:46 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/IUWMBI-599>



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 2 de 18

## ÍNDICE:

I. PROPÓSITO Y OBJETIVO: .....	3
II. ALCANCE O ÁMBITO DE APLICACIÓN: .....	3
III. MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS .....	3
IV. ROLES Y RESPONSABILIDADES.....	4
V. MATERIAS QUE ABORDA.....	6
VI. DIRETRICES DE LA POLÍTICA.....	7
VII. MECANISMO DE DIFUSIÓN.....	13
VIII. PERÍODO DE REVISIÓN.....	14
IX. EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA.....	14
X. DISTRIBUCIÓN: .....	14
XI. REFERENCIAS BIBLIOGRÁFICAS:.....	15
XII. MODIFICACIONES DEL DOCUMENTO: .....	16



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 3 de 18

## I. PROPÓSITO Y OBJETIVO

El propósito de esta política es establecer las directrices necesarias para resguardar la confidencialidad, integridad y disponibilidad de la información institucional en toda relación con proveedores y terceros que presten servicios al Hospital de Urgencia Asistencia Pública (HUAP).

El objetivo es asegurar que los contratos y convenios con proveedores incluyan cláusulas de seguridad de la información y ciberseguridad, en cumplimiento de la normativa nacional vigente y de los estándares internacionales aplicables (ISO/IEC 27001 e ISO/IEC 27002), fortaleciendo la confianza y la continuidad operativa del hospital.

## II. ALCANCE O ÁMBITO DE APLICACIÓN:

Esta política aplica a todos los proveedores y terceros que entreguen bienes o servicios al Hospital de Urgencia Asistencia Pública (HUAP), incluyendo a aquellos que tengan acceso a información institucional, sistemas, infraestructura tecnológica o recursos físicos y digitales del hospital.

Asimismo, es aplicable a todos los funcionarios y unidades del HUAP que participen en la gestión, contratación, supervisión o uso de servicios provistos por terceros.

Quedan excluidas de esta política las contrataciones de bienes o servicios que no impliquen acceso a información institucional ni a infraestructura tecnológica, tales como suministros generales que no impliquen acceso a información institucional en ningún soporte (físico o digital) ni a infraestructura tecnológica.

## III. MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- ISO/IEC 27001:2022 – Estándar internacional de gestión de seguridad de la información, que establece los requisitos para implementar un SGSI.
- ISO/IEC 27002:2022 – Código de prácticas para controles de seguridad de la información. Control 5.19: Seguridad de la información en relaciones con proveedores.
- Ley N° 21.663 (2024) – Marco de Ciberseguridad para infraestructuras críticas.



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 4 de 18

- Ley N° 19.628 (1999) – Sobre protección de la vida privada y datos personales.
- Ley N° 21.719 (2024) – Que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, con entrada en vigencia general desde el 01 de diciembre de 2026.
- Ley N° 20.285 (2008) – Acceso a la información pública.
- Ley N° 19.799 (2002) – Sobre documentos electrónicos, firma electrónica y servicios de certificación.
- Decreto Supremo N° 83 (2004) – Norma técnica sobre seguridad y confidencialidad de documentos electrónicos.
- Decreto Supremo N° 7 (2023) – Norma técnica de ciberseguridad en el marco de la Ley N° 21.180 sobre Transformación Digital del Estado.
- Orientaciones técnicas del MINSAL sobre seguridad de la información, gestión de contratos y proveedores en el ámbito hospitalario.
- Instructivo ITS-NC-006 V5.0 (2025) – “Cláusulas de Protección de Datos y Seguridad de la Información para Contratos Tecnológicos del Sector Salud”, Ministerio de Salud de Chile, aprobado mediante Resolución Exenta N° 850 del 29 de julio de 2025. Disponible en: [https://www.minsal.cl/seguridad\\_de\\_la\\_informacion](https://www.minsal.cl/seguridad_de_la_informacion)

#### IV. ROLES Y RESPONSABILIDADES.

##### Subdirección Administrativa

- Garantizar el cumplimiento de esta política en los contratos con proveedores tecnológicos.
- Coordinar la aplicación de sanciones contractuales ante incumplimientos.

##### Asesoría Jurídica

- Revisar que los contratos incluyan cláusulas de confidencialidad, protección de datos y seguridad.
- Apoyar legalmente en controversias o incidentes con proveedores.

##### Departamento de Abastecimiento

- Gestionar los procesos de adquisición y contratación de bienes y servicios con proveedores externos, asegurando la incorporación de las cláusulas de seguridad y confidencialidad establecidas en esta política.
- Aplicar las sanciones contractuales que correspondan, en coordinación con la Subdirección Administrativa y Asesoría Jurídica.



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 5 de 18

- Mantener los registros actualizados de los contratos con proveedores y de su cumplimiento en materia de seguridad de la información.

### **Unidad de Tecnología de la Información**

- Validar los requisitos técnicos de seguridad y los SLA en los contratos.
- Administrar y controlar el acceso de proveedores a sistemas e infraestructura TI.
- Monitorear el cumplimiento técnico de las cláusulas de confidencialidad y seguridad de la información establecidas en los contratos, en coordinación con el Encargado/a de Ciberseguridad y Seguridad de la Información.
- Participar en la clasificación de proveedores según su nivel de criticidad, considerando el acceso a información institucional, sistemas o infraestructura tecnológica.

### **Encargado/a de Ciberseguridad y Seguridad de la Información**

- Supervisar incidentes de seguridad relacionados con proveedores.
- Hacer seguimiento al cumplimiento de las obligaciones de seguridad.
- Reportar a la Subdirección Administrativa y al Departamento de Abastecimiento cualquier incumplimiento detectado en las cláusulas de confidencialidad o seguridad.
- Coordinar la gestión de riesgos asociados a proveedores, asegurando la identificación, evaluación y tratamiento de riesgos en materia de seguridad de la información, en conjunto con la Unidad de Tecnología de la Información y las unidades pertinentes.

### **Proveedores Externos**

- Cumplir con las cláusulas contractuales y políticas de seguridad del HUAP.
- Notificar incidentes de seguridad que afecten sus servicios o la infraestructura del hospital.

### **Personal Externo vinculado a contratos**

- Respetar las políticas de seguridad y usar los recursos sólo para fines autorizados.

### **Funcionarios del HUAP**

- Cumplir esta política en toda interacción con proveedores.
- Reportar incumplimientos o riesgos a la UTIC o al Encargado/a de Ciberseguridad y Seguridad de la Información.



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 6 de 18

## V. MATERIAS QUE ABORDA.

- La presente política regula los aspectos administrativos, técnicos y contractuales necesarios para asegurar la correcta gestión de la seguridad de la información en la relación con proveedores y terceros. En particular, aborda las siguientes materias:
- Evaluación y selección de proveedores: criterios de seguridad de la información que se deben considerar al contratar servicios o productos.
- Cláusulas contractuales de seguridad: definición e inclusión de obligaciones mínimas en contratos con proveedores que tengan acceso a información institucional, sistemas tecnológicos o infraestructura crítica.
- Clasificación de proveedores: identificación de proveedores críticos según el nivel de acceso a información, infraestructura o impacto en la operación hospitalaria.
- Gestión de riesgos asociados a proveedores: análisis y mitigación de riesgos relacionados con confidencialidad, integridad y disponibilidad de la información.
- Supervisión y monitoreo: mecanismos de control y seguimiento del cumplimiento de las obligaciones de seguridad de la información por parte de los proveedores.
- Gestión de incidentes con proveedores: procedimientos de notificación, coordinación y resolución de incidentes de seguridad que involucren a terceros.
- Confidencialidad y protección de datos personales: resguardo de la información sensible de pacientes, funcionarios y del hospital en manos de proveedores.
- Terminación de contratos y salida de proveedores: procedimientos para asegurar la devolución, destrucción o borrado seguro de información institucional al término de la relación contractual.



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 7 de 18

- Auditorías y revisiones: controles periódicos sobre proveedores para validar cumplimiento de cláusulas de seguridad.
- Mejora continua: revisión de prácticas de gestión de proveedores y actualización de la política en función de la normativa y riesgos emergentes.

## VI. DIRECTRICES DE LA POLÍTICA.

### 1. Requisitos de Seguridad en la Contratación

**1.1.** Todo contrato o convenio con proveedores deberá incluir cláusulas específicas de seguridad de la información y confidencialidad, conforme a las directrices del Ministerio de Salud establecidas en el **Instructivo ITS-NC-006, Versión 5.0 (2025)**.

#### Referencia a Cláusulas Ministeriales de Seguridad de la Información:

En cumplimiento de lo dispuesto por el Ministerio de Salud, todo contrato o convenio tecnológico deberá **incorporar o hacer referencia expresa** al documento titulado “**Cláusulas de Protección de Datos y Seguridad de la Información para Contratos Tecnológicos del Sector Salud**” (*Instructivo ITS-NC-006, Versión 5.0, aprobado mediante Resolución Exenta N° 850, de 29 de julio de 2025, MINSAL*).

Estas cláusulas constituyen el **marco obligatorio de seguridad aplicable** en materia de **confidencialidad, ciberseguridad, protección de datos personales, propiedad intelectual, continuidad operativa y gestión de incidentes**.

El documento oficial se encuentra disponible en el portal del Ministerio de Salud: [https://www.minsal.cl/seguridad\\_de\\_la\\_informacion](https://www.minsal.cl/seguridad_de_la_informacion)

#### 1.2 Incorporación obligatoria como anexo contractual:

El ITS-NC-006 del Ministerio de Salud deberá incorporarse como exigencia obligatoria en las bases y contratos de nuevas contrataciones TI que celebren las unidades competentes. Las actualizaciones o nuevas versiones del ITS-NC-006 deberán incorporarse en las contrataciones que



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 8 de 18

se inicien con posterioridad a su publicación. Respecto de contratos vigentes, la incorporación y exigibilidad de nuevas versiones se realizará conforme a las cláusulas de modificación previstas en las bases y/o el contrato y, cuando proceda, mediante el acto administrativo fundado y el anexo/modificación contractual correspondiente.

**Al menos, se deberán contemplar las siguientes obligaciones:**

- **Notificación de vulnerabilidades:** El proveedor deberá informar oportunamente toda vulnerabilidad detectada en los servicios y productos provistos, ya sea descubierta internamente o reportada por terceros.
- **Corrección de vulnerabilidades:** Ante la detección de una vulnerabilidad, el proveedor deberá entregar una solución o medida temporal que mitigue el riesgo a la mayor brevedad posible, e informar formalmente al hospital una vez implementada la corrección.
- **Notificación de incidentes de ciberseguridad:** El proveedor deberá reportar de inmediato todo incidente de ciberseguridad que afecte directa o indirectamente la infraestructura tecnológica utilizada para prestar servicios, incluso si no ha tenido un impacto aparente.

**1.3.** Los productos, servicios y soluciones tecnológicas contratadas deberán cumplir, como mínimo, con estándares básicos de seguridad: cifrado de datos, autenticación robusta y control de accesos.

## 2. Protección de Datos e Información

**2.1.** Los proveedores deberán garantizar la confidencialidad, integridad y disponibilidad de la información institucional, incluyendo datos personales de pacientes, funcionarios y terceros.

**2.2.** La obligación de confidencialidad se mantendrá vigente incluso una vez finalizada la relación contractual.

**2.3.** Está prohibido utilizar información del Hospital para fines distintos a los estipulados en el contrato.



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 9 de 18

### 3. Responsabilidades de los Proveedores

3.1. Cada proveedor será responsable de implementar las medidas de seguridad comprometidas en el contrato y en la presente política.

3.2. Los incumplimientos podrán dar lugar a la aplicación de medidas correctivas, sanciones contractuales o término anticipado del contrato. Entre ellas, se consideran:

- Amonestación formal por escrito al proveedor, con plazo definido para corregir la falta.
- No emisión del Acta de Recepción Conforme de los servicios o entregables hasta que el proveedor subsane el incumplimiento detectado.
- Aplicación de multas o penalidades económicas, de acuerdo con lo estipulado en el contrato.
- Suspensión temporal del servicio o acceso a los sistemas hasta que se restablezca la conformidad con los requisitos de seguridad.
- Terminación anticipada del contrato, en casos de incumplimientos graves o reiterados que pongan en riesgo la confidencialidad, integridad o disponibilidad de la información.
- Remisión y/o derivación de antecedentes a la Dirección de Compras y Contratación Pública (ChileCompra), solicitando evaluar la procedencia de la suspensión u otras medidas respecto del Registro de Proveedores, cuando corresponda, conforme a la normativa vigente y a los antecedentes del caso.

### 4. Notificación de Incidentes

4.1. Todo incidente de seguridad que afecte a los servicios contratados, a la infraestructura o a la información institucional deberá ser notificado de inmediato al Hospital, a través de los siguientes mecanismos:



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 10 de 18

### Canales de notificación:

- Correo institucional a la Unidad de Tecnología de la Información y al Encargado/a de Ciberseguridad y Seguridad de la Información.
- Llamado telefónico directo en casos críticos que afecten la continuidad operativa.
- Registro formal en el sistema de gestión de incidentes del Hospital (cuando aplique).

### Responsable de notificación:

El proveedor deberá designar un **punto de contacto oficial** (responsable de seguridad o coordinador técnico) para realizar la notificación.

### Plazo de notificación:

- **Incidentes críticos** (afectan operación clínica, datos sensibles o servicios críticos): notificación **inmediata (menos de 1 hora desde su detección)**.
- **Incidentes no críticos**: notificación dentro de las **24 horas siguientes**.

### Contenido mínimo del reporte inicial:

- Descripción del incidente.
- Fecha y hora de detección.
- Sistemas, servicios o datos afectados.
- Medidas iniciales adoptadas.
- Contacto del responsable del proveedor para seguimiento.

4.2. El proveedor deberá presentar un Plan de Acción Correctiva para la gestión del incidente, de acuerdo con las siguientes directrices:



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 11 de 18

### Plazo de entrega:

- Dentro de las **48 horas posteriores** a la notificación del incidente, el proveedor deberá entregar un plan preliminar.
- En un máximo de **5 días hábiles**, deberá presentar el plan definitivo con medidas correctivas y preventivas.
- **El plazo para la ejecución de las acciones correctivas** deberá establecerse en el propio Plan de Acción Correctiva, considerando la criticidad del incidente y previa validación por la Unidad de Tecnología de la Información y el Encargado/a de Ciberseguridad y Seguridad de la Información

### Canal de entrega:

- El Plan de Acción Correctiva deberá enviarse al correo institucional de la **Unidad de Tecnología de la Información y del Encargado/a de Ciberseguridad y Seguridad de la Información**.
- En casos críticos, deberá además ser registrado en el **sistema de gestión de incidentes del Hospital** (cuando corresponda).

### Formato mínimo del Plan de Acción Correctiva:

- Descripción del incidente (qué pasó y cómo se detectó).
- Análisis preliminar de causa raíz.
- Acciones inmediatas ejecutadas para contener el impacto.
- Acciones correctivas propuestas, con responsables y plazos definidos.
- Acciones preventivas para evitar recurrencia.
- Indicadores de seguimiento (ej: % de avance, fecha estimada de cierre).



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 12 de 18

### **Validación:**

El Plan de Acción Correctiva deberá ser revisado y aprobado por la **Unidad de Tecnología de la Información** y el **Encargado/a de Ciberseguridad y Seguridad de la Información**. El Hospital podrá solicitar ajustes antes de su ejecución.

### **5. Finalización de Contratos**

5.1. Al término de la relación contractual, el proveedor deberá devolver todos los activos físicos y digitales entregados por el Hospital.

5.2. El proveedor deberá revocar los accesos habilitados y eliminar de manera segura toda la información institucional bajo su custodia, debiendo acreditar dicho procedimiento al Hospital mediante las siguientes acciones:

#### **Revocación de accesos:**

- Eliminación de credenciales de usuario, llaves de acceso, tokens de autenticación o VPN utilizados para conectarse a sistemas del hospital.
- Entrega de un reporte que confirme la baja de dichos accesos, firmado por el responsable técnico del proveedor.

#### **Eliminación segura de la información:**

- Borrado seguro en medios digitales mediante técnicas reconocidas (ej. **NIST SP 800-88**, sobrescritura múltiple, cifrado seguido de destrucción de la clave).
- En caso de medios físicos (discos, respaldos, documentos impresos), destrucción certificada por métodos aprobados (triturado, desmagnetización, incineración controlada).

#### **Plazo:**



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 13 de 18

El proceso de eliminación y revocación deberá completarse en un plazo máximo de **10 días hábiles posteriores al término del contrato**, salvo que exista normativa más estricta.

## 6. Cumplimiento Normativo

6.1. Los proveedores deberán cumplir con las normativas legales vigentes en materia de protección de datos personales y ciberseguridad.

6.2. Asimismo, deberán respetar las políticas internas del Hospital y las directrices establecidas por el Ministerio de Salud.

## VII. MECANISMO DE DIFUSIÓN.

La difusión de la presente política se realizará mediante los siguientes canales:

- Envío de correo institucional a las jefaturas de áreas y unidades que gestionen o interactúen con proveedores.
- Incorporación como documento de referencia en los procesos de contratación y en la revisión de contratos por parte de la Subdirección Administrativa, Asesoría Jurídica, Departamento de Abastecimiento y la Unidad de Tecnología de la Información.
- Entrega directa a proveedores externos, cuando corresponda, al momento de formalizar contratos de servicios tecnológicos.

Asimismo, se deberá garantizar que los proveedores conozcan y acepten formalmente las disposiciones de esta política antes de la contratación.

Para ello, la Unidad de Tecnología de la Información y la Subdirección Administrativa deberán coordinar con las áreas de Abastecimiento y Asesoría Jurídica la incorporación de una cláusula de referencia en las bases de licitación, contratos o convenios, indicando expresamente que el proveedor debe dar cumplimiento a la Política de Relación con Proveedores del Hospital de Urgencia Asistencia Pública (HUAP).



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 14 de 18

Durante el proceso de licitación, la presente política deberá incorporarse como anexo a las bases de licitación publicadas, a fin de que los oferentes conozcan sus disposiciones antes de presentar sus ofertas.

En el proceso de adjudicación, se entregará copia digital a los proveedores seleccionados, quienes deberán confirmar su conocimiento y aceptación como requisito previo a la firma del contrato.

### **VIII. PERÍODO DE REVISIÓN.**

La presente política deberá ser revisada al menos cada dos años, o antes si se producen cambios normativos, tecnológicos o de gestión que lo requieran, con el fin de garantizar que:

- Mantenga su adecuación al propósito definido.
- Refleje los cambios en las tecnologías y en la gestión de proveedores.
- Se mantenga alineada con la legislación vigente, los estándares internacionales y las mejores prácticas en materia de seguridad de la información y ciberseguridad.

### **IX. EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA**

En situaciones excepcionales, el Jefe/a de la UTIC, el Encargado de Ciberseguridad y Seguridad de la Información, o el Comité de Ciberseguridad, 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.

### **X. DISTRIBUCIÓN:**

- Dirección.
- Subdirección Administrativa.



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 15 de 18

- Subdirección de Gestión Clínica.
- Subdirección de Gestión del Cuidado.
- Unidad de Calidad y Seguridad del Paciente.
- Unidad de Tecnologías de la Información.
- Asesoría Jurídica.

## X. REFERENCIAS BIBLIOGRÁFICAS:

- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
- International Organization for Standardization. (2022). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls*. ISO.
- Biblioteca del Congreso Nacional de Chile. (1999). Ley N° 19.628 sobre protección de la vida privada. <https://www.bcn.cl/leychile/navegar?idNorma=141599>
- Biblioteca del Congreso Nacional de Chile. (2008). Ley N° 20.285 sobre acceso a la información pública. <https://www.bcn.cl/leychile/navegar?idNorma=276363>
- Biblioteca del Congreso Nacional de Chile. (2024). Ley N° 21.663 que establece un marco de ciberseguridad e infraestructura crítica de la información. <https://www.bcn.cl/leychile/navegar?idNorma=1221319>
- Ministerio de Salud de Chile. (2024). Orientaciones técnicas sobre ciberseguridad y gestión de proveedores en el sector salud. MINSAL.
- Ministerio de Salud de Chile. (2025, julio 29). Instructivo ITS-NC-006 V5.0: Cláusulas de Protección de Datos y Seguridad de la Información para Contratos Tecnológicos del Sector Salud [Resolución Exenta N.º 850]. [https://www.minsal.cl/seguridad\\_de\\_la\\_informacion](https://www.minsal.cl/seguridad_de_la_informacion)



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 16 de 18

## XII. MODIFICACIONES DEL DOCUMENTO:

SÍNTESIS DE MODIFICACIONES			RESPONSABLE MODIFICACIÓN	APROBADO POR DIRECTOR
VERSIÓN	FECHA	CAUSA DE MODIFICACIÓN		
01	01/2026	Creación del Documento	Enzo Mayo Gonzalez Encargado Ciberseguridad	Dr. Patricio Barría A.



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 17 de 18

**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. TM. Camila Benítez Ugarte, Profesional Unidad de Calidad y Seguridad del Paciente
3. Christian Echeverría A, Subdirector Administrativo y Financiero



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/IUWMBI-599>

	HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA	Código: UTIC
	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	Versión: 01
	UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01/2026 Vigencia: 5 años
	POLÍTICA DE RELACIÓN CON PROVEEDORES	Página 18 de 18



Firmado por:  
Camila Andrea Benítez Ugarte  
Profesional Unidad Calidad y  
Seguridad del Paciente  
Fecha: 12-01-2026 12:50 CLT  
Hospital de Urgencia Asistencia  
Pública Dr. Alejandro del Río



Firmado por:  
Susana Ximena Avendaño Durán  
Jefatura Tic  
Fecha: 13-01-2026 11:39 CLT  
Hospital de Urgencia Asistencia  
Pública Dr. Alejandro del Río



Firmado por:  
Christian Irving Echeverría Aburto  
Subdirector Gestión Administrativa y  
Financiera  
Fecha: 14-01-2026 07:27 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/IUWMBI-599>

**II. TÉNGASE PRESENTE** la vigencia de esta política a contar de la fecha de la total tramitación de la presente Resolución.

**III. ESTABLÉCESE** que la señalada “*Política de Relación con Proveedores*”, debe ser la que se tenga en consideración a contar de la fecha de su entrada en vigencia.

**IV. DIFÚNDASE** por los canales institucionales, dejando constancia de su publicación y acceso.

**ANÓTESE, COMUNÍQUESE Y ARCHÍVESE**

CEWSP

Distribución:

1. Dirección.
2. Subdirección de Gestión Clínica.
3. Subdirección de Gestión del Cuidado.
4. Subdirección de Gestión y Administrativa y Financiera.
5. Unidad de Calidad y Seguridad del Paciente.
6. Unidad de Tecnologías de la Información.
7. Asesoría Jurídica.
8. Oficina de Partes.



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/IUWMBI-599>