	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 1 de 10

Política Acuerdos de Intercambio de Información

Octubre 2024



	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 2 de 10

Tabla de contenidos

1. Propósito	3
2. Alcance o ámbito de aplicación.....	3
3. Marco normativo.....	4
4. Roles y responsabilidades	5
5. Materias que aborda.....	5
6. Directrices de la política	6
6.1 Consideraciones generales.....	6
6.2 Seguridad de los servicios de red	6
6.3 Políticas y procedimientos de transferencia de información y software.....	6
6.3.1 Directrices generales.....	6
6.3.2 Intercambio de Información Manual	7
6.3.3 Intercambio vía correo electrónico institucional	7
6.3.4 Intercambio vía acceso remoto.....	8
6.3.5 Interoperación entre sistemas	8
6.4 Acuerdos de transferencia de información.....	8
6.5 Acuerdos de confidencialidad o no divulgación.....	9
7. Mecanismo de difusión	10
8. Excepciones al cumplimiento de la política	10

	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 3 de 10

1. Propósito

Definir las directrices para proteger el intercambio de información sensible, entre el Hospital con organizaciones externas, a través de:

- Servicios de red.
- Procedimientos de transferencia de información.
- Acuerdos de transferencia.
- Acuerdos de confidencialidad.


2. Alcance o ámbito de aplicación

Esta política se refiere a toda la información física y electrónica contenida en los sistemas de información del Hospital, que requiera ser entregada a entidades externas. Bajo las siguientes modalidades:

- Acuerdos de intercambio de información con organizaciones externas, bajo el concepto de interoperabilidad de sistemas.
- Intercambio de Información con organizaciones externas, por traspaso de información vía correo electrónico, por acceso a internet, login a otros sistemas, y/o por cualquier medio magnético o de almacenamiento, papel o medio disponible.

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Hospital Carlos Van Buren.


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

	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 4 de 10

Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Administración de activos	A.13.01.02	Seguridad de los servicios de red.
	A.13.02.01	Políticas y procedimientos de transferencia de información.
	A.13.02.02	Acuerdos de transferencia de información.
	A.13.02.03	Acuerdos de confidencialidad o no divulgación.

3. Marco normativo

- NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
- El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
 - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
 - Leyes relacionadas
- Documento del Sistema de Gestión de Seguridad de la Información, disponibles en isalud.minsal.cl.
- Ley N° 20.285, de 2008, del Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública.
 - Ley N° 19.628, de 2012, del Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada.
 - Decreto 83, de 2005, del Ministerio Secretaría General de la Presidencia, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.


	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 5 de 10

4. Roles y responsabilidades

- **Tecnologías de la Información y Comunicaciones**
 - Debe definir los mecanismos de control para la entrega e intercambio de información electrónica a entidades externas.
 - Debe disponer y aplicar medidas de protección adecuadas para el intercambio de información electrónica.
- **Encargado de Seguridad de la Información**
 - Debe auditar el cumplimiento de esta política, gestionar incidentes de seguridad que se produzcan en el intercambio de información y velar por la correcta aplicación de esta política.
- **Propietario de la información**
 - Debe autorizar o rechazar el intercambio de información de su responsabilidad.
 - Aplicar las medias de protección definidas en la presente política.
- **Usuarios**
 - **Deben cumplir con lo establecido en esta política.**

5. Materias que aborda

- Seguridad de los servicios de red.
- Políticas y procedimientos de transferencia de información.
- Acuerdos de transferencia de información.
- Acuerdos de confidencialidad o no divulgación.

	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 6 de 10

6. Directrices de la política

6.1 Consideraciones generales

El intercambio de información puede originarse en por necesidades del propio Ministerio o por requerimiento del organismo externo o incluso de un particular. En todos los casos deberá analizarse y resolver sobre las competencias del requirente para realizar tratamiento de datos de que se trate.

Todo intercambio de información electrónica perteneciente al Hospital con terceros, debe ser respaldado con un acuerdo (convenio o contrato) que incluya una cláusula de confidencialidad y/o no divulgación de la información proporcionada, en los términos de la ley 19.628 y la ley 20.584, sin perjuicio de lo señalado por la ley N° 20.285.

La operatividad del convenio o contrato le corresponde a los departamentos o áreas responsables técnicos del Hospital.

6.2 Seguridad de los servicios de red


En cualquier acuerdo de servicio de red en el hospital, el CR de Gestión de la Información debe asegurar que se incluyan mecanismos de seguridad, niveles de servicios, requisitos de administración, acuerdos de confidencialidad y derechos de auditoría. Estos requisitos se deben monitorear de manera regular para asegurar el cumplimiento de estas medidas.

Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas y redes con valor agregado y, soluciones de seguridad de redes administradas como firewalls y sistemas de detección de intrusión. Estos servicios abarcan desde la banda ancha no administrada simple a las ofertas complejas con valor agregado.

6.3 Políticas y procedimientos de transferencia de información y software

6.3.1 Directrices generales

La transferencia de información puede ocurrir a través del uso de varios tipos distintos de instalaciones de comunicación, incluido el correo electrónico, de voz y video.

	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 7 de 10

Por otro lado, la transferencia de software puede ocurrir a través de varios medios distintos, incluida la descarga de internet y la adquisición de proveedores que venden los productos listos para usar, en la medida que cumplan los estándares de seguridad requerimos para el tratamiento de datos sensibles.

Para el resguardo de la información contra malware (software malicioso), en cualquier intercambio a través de comunicaciones electrónicas, se deben llevar a cabo de acuerdo a lo definido en el “Procedimiento contra código malicioso”.

Cualquier servicio o acuerdo de transferencia de información, debe cumplir con los requisitos legales, definidos para el Sistema de Seguridad de la Información, publicado en el sitio web https://www.minsal.cl/seguridad_de_la_informacion/ y los documentos del Sistema de Gestión de Seguridad de la Información disponibles en <http://10.6.96.210/menu/login.php>

6.3.2 Intercambio de Información Manual

El intercambio de información manual sólo debe utilizar los servicios de correos autorizados en el Hospital, en forma certificada, para controlar su eventual trazabilidad. De ser entregada por mano, debe ser de forma personal al destinatario en un sobre sellado y su entrega debe quedar registrada.


6.3.3 Intercambio vía correo electrónico institucional

Toda información enviada desde el Hospital a través de correos electrónicos deberá incluir en su pie de página, una advertencia en cuanto a su uso y autorizaciones al respecto, quedando bajo responsabilidad del emisor y receptor el cuidado y resguardo de la información.

Además, la información debe ser encriptada para proteger el contenido en los mensajes de correo electrónico.

Cualquier archivo adjunto que sea enviado mediante correo electrónico, debe ser cifrado y protegido para que sólo el destinatario pueda tener acceso a la información.

Queda prohibido el reenvío automático de correos electrónicos a direcciones de correo externas.

	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 8 de 10

6.3.4 Intercambio vía acceso remoto

Todo intercambio por este medio debe cumplir con la Política de Control de acceso y Seguridad de la Red, establecidos por el MINSAL y el Hospital Carlos Van Buren.


6.3.5 Interoperación entre sistemas

Los acuerdos de interoperabilidad entre sistemas; entre el Hospital Carlos Van Buren y organismos externos, también llamados Convenios de Cooperación, deben establecer al menos: el tipo de datos que se intercambiará, las competencias de los órganos, los sistemas que interoperarán, las obligaciones, costos, incumplimientos, responsabilidades y estándares de seguridad. Los convenios tendrán vigencia desde la total tramitación de los Actos Administrativos que los aprueben.

6.4 Acuerdos de transferencia de información

Cualquier acuerdo de transferencia de información entre el Hospital y partes externas, debe abordar la transferencia segura de la información, para esto los acuerdos deben incorporar lo siguiente:

- Tipos de datos que se transfieren y finalidad autorizada.
- Competencias del requirente para requerir la información.
- administración de responsabilidades para controlar y notificar la transmisión, el despacho y la recepción.
- procedimientos para garantizar la capacidad de seguimiento y no repudiación.
- normas técnicas mínimas para el empaque y la transmisión.
- acuerdos de garantía en depósito.
- responsabilidades en caso de incidentes de seguridad de la información, como la pérdida de datos y obligación de notificación de incidentes de seguridad que afecten al sistema o a los datos.
- uso de un sistema de etiquetado acordado para la información sensible o crítica, que garantice que el significado de las etiquetas se comprenda inmediatamente y que la información se proteja adecuadamente.
- normas técnicas para registrar y leer la información y software.

	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 9 de 10

- cualquier control especial necesario para proteger elementos sensibles, como criptografía.
- mantener una cadena de custodia para la información durante el tránsito.
- niveles aceptables de control de acceso.

El contenido de información de seguridad de cualquier acuerdo debe reflejar la sensibilidad de la información involucrada.


6.5 Acuerdos de confidencialidad o no divulgación

Todo acuerdo de interoperabilidad y comunicación de datos debe contener acuerdos de confidencialidad y de no divulgación para proteger la información sensible de la organización, junto con informar a los proveedores sobre su responsabilidad al manipular información sensible.

Cuando los acuerdos de confidencialidad incluyan el acceso de terceros a información sensible o confidencial (por ejemplo, datos de pacientes), se deben considerar además los siguientes requisitos:

- una definición de la información que se protegerá (es decir, información confidencial);
- duración esperada de un acuerdo, incluidos los casos donde es posible que sea necesario mantener la confidencialidad de manera indefinida;
- acciones necesarias al terminar un acuerdo;
- responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada;
- propiedad de la información, secretos comerciales y propiedad intelectual y cómo esto se relaciona con la protección de información confidencial;
- el uso permitido de la información confidencial y los derechos del firmante para utilizar la información;
- el derecho para auditar y monitorear actividades que involucran información confidencial;
- el proceso para notificar e informar la divulgación no autorizada o la fuga de información confidencial;
- términos para la información que se va a regresar o destruir al término del acuerdo;
- medidas esperadas que se tomarán en caso de un incumplimiento del acuerdo.

En base a los requisitos de seguridad de la información, es posible que se deban incluir otros elementos en un acuerdo de confidencialidad o de no divulgación.

	Hospital Carlos Van Buren CR Gestión de la Información	CS - 004
	Política Intercambio de Información	Fecha: 24/10/2024
		Página 10 de 10

Los acuerdos de confidencialidad y no divulgación deben cumplir con todas las leyes y normativas pertinentes para la jurisdicción a la que corresponden.

7. Mecanismo de difusión

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

- Publicación en la intranet del HCVB <http://10.6.96.210/menu/login.php>
- Correo informativo.

8. Excepciones al cumplimiento de la política

Frente a casos especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente.

Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.