	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 1 de 9

Política de Seguridad de la Red

Octubre 2024



	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 2 de 9

Tabla de contenidos

1. Propósito	3
2. Alcance o ámbito de aplicación.....	3
3. Marco normativo.....	4
4. Roles y responsabilidades	4
5. Materias que aborda.....	5
6. Directrices de la política	5
6.1 Cumplimiento de la legislación	5
6.2 Definiciones asociadas a la Seguridad de las Telecomunicaciones.....	5
6.3 Lineamientos mínimos en Seguridad de las Telecomunicaciones	6
6.3.1 Gestión en controles de red.....	6
6.3.2 Gestión en seguridad de los servicios de red.....	6
6.3.3 Gestión en separación y segmentación de las redes.	6
6.3.4 Gestión en protección en la transferencia de información	7
6.3.5 Gestión en mensajería electrónica.....	7
6.3.6 Gestión en redes inalámbricas	7
6.3.7 Gestión de auditorías	8
6.3.8 Gestión en Acuerdos de confidencialidad o no divulgación	8
6.3.9 Aseguramiento de servicios de aplicación en redes públicas	8
7. Mecanismo de difusión	9
8. Excepciones al cumplimiento de la política	9

	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 3 de 9

1. Propósito

Esta Política de Seguridad de las Telecomunicaciones, establece los lineamientos para maximizar la efectividad de la operación informática, garantizando la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.

Mantener la seguridad de la información transferida dentro de la institución y con cualquier entidad externa.

2. Alcance o ámbito de aplicación


Contempla la seguridad de todas las telecomunicaciones que se requiere establecer en las redes internas y las establecidas con entidades externas al Hospital.

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 – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 4 de 9


Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Control de acceso	A.09.01.02	Accesos a las redes y a los servicios de la red.
Seguridad de las comunicaciones	A.13.01.01	Controles de red
	A.13.01.02	Seguridad de los servicios de red
Adquisición, desarrollo y mantenimiento del sistema	A.14.01.02	Aseguramiento de servicios de aplicación en redes públicas

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
- Documentos relacionados:
 - Procedimiento gestión de derechos de acceso y devolución de activos.
 - Política control de acceso.
 - Política protección de mensajes electrónicos.

4. Roles y responsabilidades

- **Jefe Tecnologías de la Información y Comunicaciones**
 - Debe disponer los controles y reglas de control de acceso.
 - Autorizar los mecanismos de control para los dominios de seguridad definidos.
 - Aprobar medidas de control para las excepciones que permitan acceso directo desde dominios “No Confiables” hacia servidores de producción.
- **Encargado de Seguridad de la Información**
 - Coordinar mecanismos de control para los dominios de seguridad definidos.

	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 5 de 9

- **Infraestructura TIC**
 - Es responsable de la aplicación operativa de esta política.

5. Materias que aborda

- Accesos a las redes y a los servicios de la red.
- Controles de red.
- Seguridad de los servicios de red.
- Aseguramiento de servicios de aplicación en redes públicas.

6. Directrices de la política


6.1 Cumplimiento de la legislación

Las medidas de control de acceso a la información definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos en el documento “Normativa del Sistema de Gestión de Seguridad de la Información”.

6.2 Definiciones asociadas a la Seguridad de las Telecomunicaciones

Las siguientes definiciones son específicas para el ámbito de seguridad de las telecomunicaciones:

- **SLA:** es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio en aspectos tales como: tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.
- **WPA2:** es un sistema para proteger las redes inalámbricas (Wi-Fi) que utiliza la versión certificada del estándar 802.11i. Fue creado para corregir las deficiencias del sistema previo, WPA que carecía de algunas características de seguridad que exigía el estándar mencionado.
- **Red inalámbrica:** se refiere a la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica. En este tipo de red, la transmisión y la recepción se realizan a través de puertos.

	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 6 de 9

6.3 Lineamientos mínimos en Seguridad de las Telecomunicaciones

6.3.1 Gestión en controles de red.


- Las redes se deben gestionar, controlar su acceso y uso, para proteger la información contenida en los sistemas y aplicaciones.
- Todos los usuarios que accedan a la red deben contar con una identificación individual única.
- Todo acceso a servicios críticos debe ser validado y todo intento, exitoso o fallido, debe ser registrado para su análisis posterior.
- La red debe restringir accesos riesgosos, tales como:
 - Mensajería instantánea.
 - Descarga de archivos desde sitios peer to peer.
 - Acceso a sitios de pornografía.
 - Conexiones a sitios de streaming no autorizados.

6.3.2 Gestión en seguridad de los servicios de red

- Los mecanismos de seguridad, los niveles del servicio (SLAs) y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios sean prestados en forma interna o por terceros.
- Los puertos de configuración y de diagnósticos de los dispositivos de la red de comunicaciones deben ser protegidos de accesos no autorizados.

6.3.3 Gestión en separación y segmentación de las redes.

- Se deben identificar los dominios o zonas de seguridad requeridos en la arquitectura de la red de telecomunicaciones, permitiendo de esta forma establecer distintos niveles de confianza.
- No se deben permitir accesos directos entre dominios no confiables, hacia un ambiente productivo.

	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 7 de 9

- Los grupos de servicios de información, usuarios y sistemas de información se deben separar en dominios o zonas de seguridad según su criticidad para la institución.

6.3.4 Gestión en protección en la transferencia de información


- Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación necesarias.
- Los acuerdos deben considerar la transferencia segura de la información del negocio entre la organización y terceros. Este tipo de conexiones, deben ser monitoreadas mediante procesos definidos y controlados por revisiones periódicas.
- Se deben señalar los niveles de protección adecuada al nivel de sensibilidad de la información transferida, acordando, por ejemplo, necesidad de cifrado y/o firma digital para la transferencia.

6.3.5 Gestión en mensajería electrónica

- Se debe establecer una política particular de acceso y uso del sistema correo electrónico institucional (ver política de protección de mensajes electrónicos).
- La información involucrada en la mensajería electrónica debe ser debida y adecuadamente protegida.

6.3.6 Gestión en redes inalámbricas

- La incorporación de redes inalámbricas no debe afectar el nivel de seguridad de la red de la Institución y su acceso a las restantes redes debe ser controlado con el equipamiento que resulte necesario.
- Las contraseñas a utilizar deben ser WPA2 o superior, con una composición robusta y cambiadas de acuerdo con el estándar definido por la Institución.
- Se debe mantener una nómina de estos accesos inalámbricos, con sus contraseñas, ubicación y usuarios que la utilizan frecuentemente.
- Estas redes deben constituir un dominio separado de las otras redes de la Institución, cuidando que su alcance no cubra zonas que queden fuera de su control.
- Se debe establecer un sistema de monitoreo permanente de estas redes inalámbricas, con la capacidad de alertar de eventos sospechosos.

	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 8 de 9

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

6.3.7 Gestión de auditorías


- Se deben establecer revisiones periódicas de cumplimiento de los controles definidos y establecidos, para asegurar la protección contra el acceso de personas no autorizadas.
- El Encargado de Seguridad de la Información / Encargado de Ciberseguridad son responsable de establecer revisiones periódicas de cumplimiento de los controles definidos, con el fin de proteger el acceso de personas no autorizadas.

6.3.8 Gestión en Acuerdos de confidencialidad o no divulgación

- Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de protección de la información de la Institución.
- Se debe generar por la institución, acuerdos de confidencialidad o NDA (non disclosure agreement), documento base para cada tipo de acuerdo con terceros.

6.3.9 Aseguramiento de servicios de aplicación en redes públicas

- La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada.

	Hospital Carlos Van Buren CR Gestión de la Información	CS – 007
	Política de Seguridad de la Red	Fecha: 24/10/2024
		Página 9 de 9

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.