Política de Seguridad Física y Ambiental

Octubre 2024

Tabla de contenidos

1. Propósito

El propósito de esta Política es establecer directrices y requisitos para los perímetros de seguridad, controles de ingreso y protección física, con el fin de resguardar las áreas donde se almacena o procesa información sensible, o existan medios de procesamiento de información.

Además, se busca prevenir la pérdida, los daños, el robo o el compromiso del equipamiento, así como la interrupción a las operaciones de la organización.

Se incluye en esta política el resguardo y trasporte de las fichas clínicas físicas (en papel).

2. Alcance o ámbito de aplicación

La Política es aplicable a todos los funcionarios de planta, contrata, honorarios, consultores, practicantes y otros trabajadores, incluyendo las empresas que presten servicios en las dependencias y oficinas del Hospital Carlos Van Buren.

Esta política abarca los siguientes controles definidos en la norma NCh-lSO 27002:2013. Controles de seguridad de la información:

- A.II.OI.OI Perímetro de seguridad física
- 11.01.02 Controles de acceso físico
- 11.01.04 Protección contra amenazas externas y del ambiente
- 11.01.05 Trabajo en áreas seguras
- A.11.01.06 Áreas de entrega y carga
- A.11.02.01 Ubicación y protección del equipamiento
- A.11.02.02 Elementos de soporte
- A.11.02.03 Seguridad en el cableado
- 11.02.04 Mantenimiento del equipamiento
- 11.02.07 Seguridad en la reutilización o descarte de equipos
- A.11.02.08 Equipo del usuario desatendido
- A.11.02.09 Política de escritorio y pantalla limpios (como referencia externa)
- A.08.03.03 Transferencia de medios físicos

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:
    - Ley N° 19.628, de Protección de vida privada y datos personales.
    - Ley N° 19.799, de firmas y documentos electrónicos. Ley N O 19.927, de Delitos de Pornografía Infantil.
    - Ley N° 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
    - Ley N° 21.180, de Transformación Digital del Estado.
    - Ley N° 21.459, que Establece normas sobre Delitos Informáticos, deroga la Ley N O 19.223 y modifica otros cuerpos legales con el Objeto de Adecuarlos al Convenio de Budapest.
    - Decreto N O 83, 2004, Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
    - Decreto Supremo 47, del Ministerio de Vivienda y Urbanismo, Ordenanza general de la ley General de Urbanismo y construcciones".
    - Decreto 594, del Ministerio de Salud "Reglamento sobre condiciones sanitarias y ambientales básicas en los lugares de trabajo"
    - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad
    - Leyes relacionadas.

- Documentos relacionados:
    - Política de pantallas y escritorios limpios.
    - Procedimiento de gestión de identidad y derechos de acceso.

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.

- **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.

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.
- 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.

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.

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.