Política de Teletrabajo

Octubre 2024

Tabla de contenidos

1. Propósito

El objetivo de la Política es establecer medidas de seguridad que protejan la información a la que se accede, procesa o almacena en sitios de trabajo a distancia o de teletrabajo, garantizando la seguridad de todos los recursos gestionados en estas condiciones, y sensibilizando a las personas sobre la importancia de cumplir con las medidas de seguridad tanto dentro como fuera de la oficina.

2. Alcance o ámbito de aplicación

Esta política 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. que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la Institución. También se aplica a todas las personas que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la Institución y se extiende a cualquier relación con terceros que implique el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea "presencial", "a distancia", "teletrabajo" u otra, en las condiciones que establezca la legislación vigente, los dictámenes de la Dirección del Trabajo, Contraloría General de la República o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta Política abarca el siguiente control definido en la norma NCh-lSO IEC 27002:2013. Controles de seguridad de la información:

- 6.2.2 Teletrabajo.

3. Marco normativo

- NCh-lS027001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información — Requisitos.
- Ley N O 19.628, de Protección de vida privada y datos personales.
- Ley N O 19.799, de firmas y documentos electrónicos.
- Ley N O 19.927, de Delitos de Pornografía Infantil.
- Ley N O 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 O 21.180, de Transformación Digital del Estado.
- Ley N O 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, de 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 N O 1, de 2015, Ministerio Secretaría General de la Presidencia, que Aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado.
- Decreto N 0 273, de 2022, Ministerio del Interior y Seguridad Pública, que Establece obligación de reportar incidentes de ciberseguridad.

4. Terminología

- **Trabajo a distancia**: Se entenderá por modalidad de trabajo a distancia aquel pacto que faculta al trabajador a prestar sus servicios total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos o instalaciones de la institución.
- **Teletrabajo**: Se entenderá por teletrabajo cuando los servicios sean prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o bien cuando los servicios prestados deban reportarse mediante tales medios. El teletrabajo se refiere a todas las formas de trabajo fuera de la oficina, incluidos los ambientes de trabajo no tradicionales, como los que se conocen como entornos de "tele conmutación", "lugar de trabajo flexible", "trabajo remoto" y "trabajo virtual".
- **Información**: Conjunto de datos que organizados en determinado contexto tienen significado o importancia.
- **Nivel de Clasificación**: De acuerdo con nivel de confidencialidad.

- **Secreto**: Aquellos, documentos e información clasificada como secreta de conformidad a esta Política, y la individualización del acto o resolución en que conste tal calificación, no pueden ser divulgados.
- **Reservado**: Información sensible, de uso exclusivamente interno. Su divulgación podría implicar un impacto no deseado para el Hospital o la transgresión de la normativa vigente. Debe ser declarada como reservada considerando la Ley N° 20.285.
- **Pública**: Toda aquella información que el Hospital genere, obtenga, o controle; y corresponde a datos que son de acceso público, y por lo tanto, no tienen requerimientos de Confidencialidad.
- **Uso Interno**: Es toda información que no contiene datos sensibles, que puede encontrarse en proceso de construcción, y que está disponible para todos los funcionarios y terceros autorizados. Esta información puede ser entregada al público sujeto a normativa vigente, previa consulta al propietario del activo de la información.

5. Roles y responsabilidades

- **Jefe de Unidad, Servicio o Centro de Responsabilidad**
  - Asegurar la aplicación y cumplimiento de las políticas, procedimientos e instructivos de seguridad de la información al interior de cada división, departamento, subdepartamento, sección o unidad según corresponda.

- **Recursos Humanos**
  - Llevar un registro de las personas que, por su perfil o condición dentro de la institución o las características de sus funciones, tienen la opción de teletrabajar.

- **Funcionarios**
  - Dar cumplimiento a las directrices establecidas en la presente Política, referidas a las acciones permitidas y prohibidas bajo el marco de las funciones de teletrabajo que le fueron encomendadas.

  - Reportar los incidentes de seguridad detectados en el ámbito del uso de autenticación secreta e informar inmediatamente cualquier pérdida, robo, daño o incidente de seguridad relacionado a su Jefatura directa y al Departamento TIC.

- **Encargado de Seguridad de la Información**
    - Velar por la implementación de las políticas de seguridad de la información al interior de la institución, de su control, de su correcta aplicación y del estricto cumplimiento de la legislación vigente.

6. Materias que aborda

- Obligaciones de usuarios en Teletrabajo.
- Medidas de seguridad.
- Tratamiento de información confidencial.

7. Directrices de la política

7.1 Medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia o de teletrabajo

- La activación del trabajo remoto deberá estar previamente autorizada y en cumplimiento con las instrucciones normativas del área de Gestión de Personas de la institución, con su equipamiento de trabajo debidamente asignado o acogiendo a BYOD - que se refiere a que se le permita usar un dispositivo de propiedad persona.

7.2 Entorno físico para teletrabajo

La persona autorizada para trabajar a distancia o teletrabajar deberá implementar las siguientes medidas:

- Habilitar una zona dentro de su hogar con suficiente espacio para contener los equipos y materiales de trabajo.
- Aislar los ruidos externos y los propios de la casa
- Controlar la iluminación, temperatura y ventilación de lugar definido.
- Es conveniente disponer de luz natural, esta disminuye el riesgo de fatiga visual.
- Evitar consumir alimentos y líquidos cerca del su equipo, podría dañarlo.
- Evitar cableado eléctrico suelto, fíjelo cosa de evitar accidentes.

- Utilizar pausas de trabajo para consumir alimentos.
- Si siente cansancio o pérdida de concentración realice un descaso.
- El equipo no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo.
- En ningún caso se debe descuidar el portátil si se viaja en transporte público. Tampoco se debe guardar en el coche ni dejarlo visible o fácilmente accesible.
- Si se trabaja en lugares donde no se garantiza la custodia del equipo, este debe quedar anclado con un candado de seguridad o guardado en un armario de seguridad.
- En caso de robo o pérdida del equipo, se debe notificar de manera inmediata al personal técnico responsable.

7.3 Obligaciones de los usuarios con Teletrabajo

A modo de "mejores prácticas" se promueve implementar las siguientes medidas de seguridad, asociadas al uso de computadores utilizados bajo modalidad de trabajo a distancia o teletrabajo:

- Usar protector de pantalla con clave cuando el computador no esté en uso.
- No dejar Pendrive/Flash Drive sin supervisión en los computadores.
- Establecer medidas para evitar el acceso de forma fortuita a información institucional por otros usuarios del equipo del funcionario, como familiares o amigos.
- Priorizar el uso de dispositivos corporativos, ya que cuentan con las políticas de seguridad que la institución considera necesarias y tienen instalado el software para realizar el trabajo de forma segura.
- Cuidar los equipos informáticos y los elementos de trabajo, que la institución ponga a su disposición para el ejercicio de sus funciones y usarlos exclusivamente con los fines laborales que se hayan fijado previamente.
- El uso de dispositivos personales debe utilizar las configuraciones y conexiones permitidas y seguras al teletrabajar desde sus dispositivos personales.
- Dar uso adecuado y responsable de la cuenta de correo electrónico que la institución le proporciona para el desarrollo de sus labores, absteniéndose de darle un uso diferente al determinado.
- Los usuarios deben permanecer alerta respecto a correos electrónicos fraudulentos. Ante cualquier duda o sospecha del funcionario sobre una amenaza, Phishing o malware, contactarse con el encargado de ciberseguridad/TI/soporte.
- Cuando en conexión a internet no sea posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utilizar la red de datos móvil 4G o 5G y siempre evitar la conexión a redes wifi-públicas.

- Evitar navegar por sitios desconocidos y abstenerse de recolectar o distribuir material ilegal a través del internet.
- De utilizar un equipo compartido en el hogar, debe crear un perfil nuevo específico para trabajar, y abstenerse de permitir su uso y acceso al sistema de personas distintas. Mantenga su antivirus actualizado y realice revisiones periódicas (diarias) de su equipo para asegurar que esté actualizado (antivirus y sistema operativo).

7.3.1 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.

7.3.2 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.

7.3.3 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.

7.3.4 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.

7.3.5 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.

7.3.6 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.

7.3.7 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.

7.3.8 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.

7.3.9 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.

8. 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.

9. 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.