# INSTRUCTIVO DE SEGURIDAD PARA ACTIVACIÓN DE TELETRABAJO Y PROTECCION DE LA INFORMACIÓN DEL HOSPITAL

Unidad de Gestión Tecnologías de la Información y Comunicaciones

HOSPITAL
SAN JUAN DE DIOS DE
LA SERENA

# I. INTRODUCCIÓN

En el contexto de la Resolución Exenta N°182, del 17.03.2020, que establece la modalidad de trabajo para funcionarios y funcionarias de las Divisiones del Ministerio de Salud, Gabinetes y Seremis de Salud, en el marco del brote de COVID-19, en específico sobre el cumplimiento estricto de las Políticas de Seguridad de la Información Institucional y medidas adicionales que determine el Departamento Tecnologías de la Información y Comunicaciones del Ministerio de Salud. Departamento que ha activado todos sus protocolos internos, siguiendo las instrucciones y recomendaciones que han hecho sobre la materia el Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior y la Contraloría General de la República. A continuación, les invitamos a seguir y cumplir atentamente las siguientes instrucciones.

# II. ALCANCE

Este documento aplica para los funcionarios del Hospital que tengan la obligación o necesidad de cumplir con sus funciones a distancia, o por condiciones de salud personal
o general que les impidan presentarse en sus puestos de trabajos.

# III. INSTRUCCIONES DE SEGURIDAD

## 1. POLITICAS

- Lea y acate las políticas de seguridad disponibles en: el link http://isalud.minsal.cl/ministerio/dgstic/SGSI/Paginas/default.aspx.

## 2. CONTRASEÑAS

- No comparta sus contraseñas.
- No utilice la misma contraseña para todos los sistemas o sitios.
- Utilice contraseñas seguras, que cumplan a lo menos con los siguientes requisitos:
  - Debe contener 8 caracteres como mínimo.
  - No debe contener: los nombres o apellidos del funcionario, el nombre de usuario, el nombre de la institución (MINSAL por ejemplo) o unidad funcional (SSP por ejemplo).
  - No debe contener palabras completas.
  - Contener al menos un carácter de las siguientes categorías.

| CATEGORIA | EJEMPLO |
|---|---|
| Letras mayúsculas | A, B, C, … |
| Letras minúsculas | a, b, c, … |
| Números | 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 |

Ejemplo de contraseñas segura: S3gur1d4d; R0ckyB4lb04

## 3. ESTACIONES DE TRABAJO

- Cierre la sesión al ausentarse o dejar de utilizar el equipo o sistema informático.
- Si debe abandonar su puesto de trabajo, aunque sea momentáneamente, bloquee su computador:
  - Tecla Windows + L
  - Control + Alt + Supr

## 4. INFORMACIÓN EN PAPELES O MEDIOS REMOVIBLES

- Guarde bajo llave en gabinete o mobiliario seguro, cuando no se esté utilizando la información.
- Deje su lugar de trabajo en orden, apague los equipos y guarde en un lugar seguro los documentos o medios removibles, al finalizar la jornada laboral.

- Retire los documentos de las impresoras inmediatamente una vez impresos.

## 5. PROTEJA LA INFORMACIÓN Y SUS MEDIOS DE ALMACENAMIENTO

- Almacene la información institucional SÓLO en servidores, estaciones de trabajo o equipos portátiles asignados por la UTIC.
- NO almacene información personal en los equipos indicados en punto anterior.
- Los equipos personales no son alternativa de almacenamiento de información del Hospital.

## 6. NAVEGACIÓN SEGURA (USO DE INTERNET)

- Utilizar exclusivamente para temas de trabajo.
- Utilice un navegador seguro.
- No acceda a sitios desconocidos o no confiables.
- No descargue archivos de sitios web no confiables.
- No debe aceptar la instalación automática de software.
    - No ejecutar archivos desde sitios dudosos.
    - No hacer click en el botón “ejecutar”.
- Tenga cuidado con las conexiones WI-FI: las conexiones abiertas o sin contraseña son peligrosas. Ajuste la configuración de sus equipos (notebook o smartphone), para evitar conectarse a redes desconocidas.
- Siempre descargue archivos en una carpeta y analícelos con un antivirus actualizado antes de abrirlos.
- No ingrese información crítica, sensible o personal en formularios, páginas o foros.
- Sólo navegue por sitios seguros (la dirección debe comenzar por https o el navegador debe indicar que es seguro)
- No almacena contraseñas en los navegadores.

## 7. ELIMINACIÓN SEGURA DE LA INFORMACIÓN

- Destruir los documentos impresos con información sensible antes de desecharlos y eliminar la información digital con herramientas adecuadas.

## 8. CORREO ELECTRÓNICO

- Revisar los correos recibidos entes de abrirlos (remitentes y asunto).
- No acceda a enlaces sospechosos o descargar archivos adjuntos de remitentes desconocidos.

## 9. CONECCIONES EXTERNAS

### a. ACCESO A LA RED, INFORMACIÓN Y SISTEMAS DEL MINISTERIO

Si necesita tener acceso a la red interna de la Institución:

- Se establece como una conexión remota segura a la red de comunicaciones Ministerial, las que se realicen a través de VPN, ya que esta conexión brinda una extensión de la red institucional a través de una red pública, y las necesarias configuraciones de seguridad para establecer un método seguro de conexión de manera remota.
- Las peticiones de VPN serán canalizadas mediante el sistema de ticket, y serán analizadas caso a caso.

- Deberá considerar que **NO necesita conexión de VPN** para los siguientes casos:
  - Correo electrónico, dado que es posible acceder vía internet por medio del siguiente enlace: https://mail.minsal.cl/, al cual podrá acceder con su correo institucional y su clave de acceso (la cual es la misma con la cual tiene configurado su acceso a Outlook, en su computador de trabajo).
  - Sistemas con acceso público; SIS-Q, Sigfe, Pukkan.cl/soporte, SIGGES, SIAPER, Correo institucional, CITO WEB, Medipass, RNI, SIGTE, SURVIH, SICARS, SIDOT, UGCC, UGCQ.
  - Es condicional esencial que para realizar tele-trabajo el PC no puede ser llevado al Hogar.

**ACCESO A MEDIOS DE COMUNICACIÓN**

Si requiere acceso a medios de comunicación para la realización de sus labores, el Ministerio de Salud cuenta con las siguientes herramientas a las que deberá hacer uso:

- Para la conexión al correo electrónico institucional a través de una red pública, deberá realizarse a través de la webmail institucional al link https://mail.minsal.cl/
- Para la necesidad de reuniones de trabajo vía video conferencia, deberá considerar el licenciamiento Zoom Meetings habilitado para cada servicio.
- Este Ministerio no se hace responsable de la calidad y privacidad de las comunicaciones que se establezcan bajo otras vías de Video Conferencia.

**c. ESTACIONES DE TRABAJO**

- Utilizar equipos institucionales con los resguardos de seguridad correspondientes. De no ser posible, el usuario deberá utilizar su equipo personal y, en conjunto con la institución, deberá verificar que su dispositivo se encuentre en condiciones de seguridad aptas: antivirus reconocido y actualizado, sistema operativo debidamente licenciado y con sus parches al día, y aplicaciones debidamente licenciadas y actualizadas.
- Establezca medidas para evitar el acceso de forma fortuita a información institucional por otros usuarios del equipo del funcionario, como familiares o amigos.

## 10. RECOMENDACIONES RESPECTO A USUARIOS REMOTOS

- Evitar conectarse a internet desde Wi-Fi público a la red institucional.
- Deberá permanecer alerta respecto a correos electrónicos fraudulentos, ya que se ha constatado un aumento de Phishing y spear Phishing en el último tiempo.
- **Si se utiliza un equipo compartido en el hogar, crear un perfil nuevo específico para trabajar**.
- Establecer medidas para evitar el acceso de forma fortuita a información institucional por otros usuarios, como familiares o amigos.
- Tener equipos de conexión remota fuera de la oficina con softwares y sistema operativo actualizados.
- Tener equipos de conexión remota fuera de la oficina con software antivirus.

## 11. INCIDENTES DE SEGURIDAD

- Ante un incidente de Seguridad de la Información, contactar inmediatamente antuan.rodriguez@redsalud.gov.cl
- Se entenderá como incidente de seguridad todo evento sospechoso o incidentes que puedan comprometer la información sensible de MINSAL.

Ante dudas técnicas para la implementación de alguna de estas medidas, contactar a antuan.rodriguez@redsalud.gov.cl.