Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

Protocolo Trabajo Remoto

Comité de Seguridad de la Información

Diciembre - 2020

Protocolo Trabajo Remoto

Comité de Seguridad de la Información

Producto de la pandemia se ha presentado la posibilidad de **trabajar a distancia**, lo que conlleva un **conjunto de riesgos** que puedan afectar la integridad, confidencialidad y disponibilidad de los activos de información de la Institución, que esperamos minimizar.

Entendiendo que no existe un medio ambiente libre de estas amenazas, debemos tomar las medidas para realizar un trabajo remoto reforzando la seguridad.

Basado en el protocolo del equipo de respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT (Sigla en inglés Computer Security Incident Response Team), y considerando nuestra realidad, el Comité de Seguridad de la Información entrega guías para el correcto y adecuado uso del sistema de acceso de Red Privada Virtual (VPN) el que será aplicable a todos los funcionarios/as de planta y/o contrata, servidores a honorarios, y a cualquier otro prestador de servicios contratado por la Subsecretaría de Justicia.

Recomendaciones a Funcionarios/as

Protocolo Trabajo Remoto | Comité de Seguridad de la Información

1.- La **contraseña de autenticación** asignada nunca deberá ser divulgada a terceros, y siempre debe ser mantenida en secreto.

2.- Es necesario **configurar el protector de pantalla y la contraseña de entrada del equipo donde instalará la VPN** de forma que, si deja libre por un momento su estación de trabajo, otra persona no tendrá acceso a los recursos de la red institucional del ministerio.

3.- Cada usuario/a que cuente con un acceso VPN, debe **asegurarse de desconectar la conexión VPN** una vez concluida las operaciones.

4.- No se debe utilizar la cuenta de acceso VPN a través de conexiones de **redes Wi-Fi de acceso público**.

5.- Siempre debe existir **cuidado y precaución extrema frente a correos electrónicos de orígenes desconocidos o fraudulentos**, apertura o acceso a páginas web de dudosas características y/o uso de redes sociales en que por medio de estas se intente vulnerar la seguridad de la red institucional.

6.- Los/as funcionarios/as, **deben revisar permanentemente el Link Intranet - Seguridad de la Información** (link), para que estén actualizados/as en materias de seguridad de la información, así como las políticas de seguridad de información interna, entre otros.

7.- Dentro de las medidas recomendables **está la creación de un perfil nuevo específico** para la ejecución de las actividades de trabajo en la red institucional.

Recomendaciones a Funcionarios/as

Protocolo Trabajo Remoto | Comité de Seguridad de la Información

8.- Se sugiere mantener los equipos con softwares y sistema operativo **actualizados**.

9.- Los equipos personales deben estar provistos con **software Antivirus instalado** (*opciones gratuitas: Avast Free Antivirus, AVG Free Antivirus, Avira Free Antivirus, Bitdefender Antivirus Free, Windows Defender*) y actualizarlos en forma rutinaria.

10.- La manipulación de archivos o elementos de información que el/la usuario/a realice, se deben mantener siempre dentro de la **conexión VPN** y se ejecutará **a través de herramientas de escritorio remoto**, manteniendo los archivos y activos de información siempre dentro de la red institucional y nunca almacenados en los equipos externos.

11.- Los usuarios **no pueden instalar software institucional en equipos personales**. Estos deben ser instalados en equipos institucionales o ingresar a través de escritorio remoto por VPN.

12.- Se debe 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.

13.- Los usuarios de una cuenta de conexión VPN con acceso a la red ministerial, una vez que retornen a las funciones 100% presenciales, deberán dar aviso a la Unidad de Informática, a fin de revocar la autorización de acceso. Para mayor información se recomienda revisar el siguiente **link**.

Recomendaciones a Jefaturas

Protocolo Trabajo Remoto | Comité de Seguridad de la Información

Cada jefatura deberá evaluar la pertinencia de solicitar acceso a VPN (Red privada virtual por sus siglas en inglés) a los/as integrantes de su equipo, priorizando el uso de web mail institucional como herramienta para trabajar de forma remota.

Cabe mencionar, que, si bien es posible configurar y habilitar las cuentas de usuarios/as de todos los/as funcionarios/as de la Subsecretaría de Justicia, debe hacerse hincapié en que **este acceso estará destinado "solo" a los/as funcionarios/as que, por su función, requieren hacer uso exclusivo de los recursos disponibles en la red informática del Ministerio** (Carpetas Compartidas, Acceso a Sistemas Internos de cada unidad, entre otras).

Por motivos de seguridad y disponibilidad de recursos de anchos de banda, **no es recomendable que este servicio sea entregado a todos los/as funcionarios/as de la Subsecretaría de Justicia**, sino que, solo a los/as funcionarios/as de planta y/o contrata, servidores a honorarios, y a cualquier otro prestador de servicios contratado por la Subsecretaría de Justicia que deben desempeñar funciones o cumplir compromisos institucionales, que no puedan resolverse mediante correo electrónico.

Comité Seguridad de la Información.

Diciembre de 2020

Ministerio de Justicia y Derechos Humanos

Gobierno de Chile