CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

PROTOCOLO DE SEGURIDAD PARA TRABAJO A DISTANCIA

El trabajo a distancia ofrece muchas ventajas, pero no está libre de riesgos de seguridad, especialmente si se trata de compartir información entre un grupo de trabajo. Para realizar esta labor de forma remota, debemos tomar algunas medidas que permitan replicar las condiciones mínimas de ciberseguridad.

ANTE EL AUMENTO DE CASOS POR CORONAVIRUS
y preocupados por apoyar el teletrabajo, el equipo del CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática), entrega las siguientes recomendaciones:

1.-

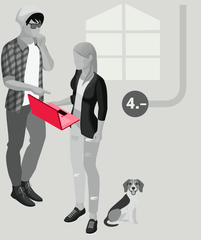
Evitar conectarse a internet desde una Wi-Fi pública a la red institucional.

Estar alerta a correos electrónicos fraudulentos, ya que en estas situaciones de emergencia, aumentan los fraudes como phishing o malware.

2.-

3.-

Revisar las políticas de seguridad de información interna de tu organización, como uso de los dispositivos móviles, de los equipos personales o la política de escritorio limpio, entre otros.



4.-

Si se utiliza un equipo compartido en el hogar, crear un perfil nuevo específico para trabajar y evitar que otros usuarios accedan a la información institucional, como familiares o amigos.

5.-

Actualizar el antivirus, softwares y sistemas operativos.

6.-

Establecer canales de comunicación oficiales para la comunicación del equipo de trabajo, soporte y jefatura.

Respaldar la información.

7.-

8.-

Acordar los horarios de trabajo, los servicios a los que se necesita tener acceso a la información y las labores que se deben desempeñar.

PARA ACCEDER AL PROTOCOLO COMPLETO, INGRESA A NUESTRO SITIO WEB
WWW.CSIRT.GOB.CL