BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

TRABAJO DESDE CASA:

MEDIDAS DE CIBERSEGURIDAD PARA HACER HOME OFFICE

BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

INTRODUCCIÓN

En los últimos años muchas empresas y organizaciones han implementado el modo de trabajo a distancia, más conocido como "home working" o "home office". Esto resulta posible gracias al amplio **avance de la tecnología que nos permite realizar nuestras tareas de todos los días desde distintos sitios**, pudiendo prescindir de estar presentes físicamente en nuestros lugares de trabajo.

Sin embargo, **esta ventaja viene acompañada de potenciales riesgos a nivel de seguridad informática** los cuales deben ser contemplados correctamente. Es importante destacar que actualmente **el "home office" es una oportunidad para el cibercriminal para causar algún tipo de daño digital**.

Según los especialistas, el 99% de los ataques comienza con alguno de los siguientes vectores: el correo electrónico (phishing) o una vulnerabilidad (es decir explotar algún error).

En tal sentido, en este material didáctico ofrecemos una serie de sugerencias y recomendaciones a implementar de manera integral a los fines de **aprovechar al máximo la posibilidad de trabajar a distancia de forma segura**.

LOS ATAQUES CIBERNÉTICOS PUEDEN TENER COMO OBJETIVO DAÑAR SISTEMAS, ROBAR INFORMACIÓN O BLOQUEAR SERVICIOS.

Los ciberatacantes aprovechan cuando las organizaciones bajan sus defensas, es por esto que se deben tomar algunos recaudos a la hora de trabajar desde casa.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

RECOMENDACIONES PARA LOS USUARIOS EMPLEADOS

EN CASO DE ESTAR UTILIZANDO DISPOSITIVOS ELECTRÓNICOS INSTITUCIONALES

CONECTIVIDAD:

- **Siempre utilizá conexión VPN** (Red Privada Virtual): te permite el acceso seguro a la red propia de tu trabajo utilizando la conexión a Internet de tu casa. Esto evita que el tráfico sea interceptado por un ciberatacante.
- **Evitá conectarte a Internet desde redes Wi-Fi públicas** como las de un bar o espacio de coworking.
- **Verificá tu Wi-Fi hogareño:** controlá que tu router posea una contraseña WPA2 y cambiala regularmente.

ES IMPORTANTE TENER EN CUENTA QUE TODO DISPOSITIVO QUE SE CONECTE A INTERNET ES POTENCIALMENTE VULNERABLE A SUFRIR UNA INFECCIÓN POR MALWARE.

CONTRASEÑAS Y CONFIGURACIONES DE SEGURIDAD:

- **Configurá una contraseña o activá datos biométricos para acceder al dispositivo**. Este último siempre se debe bloquear cuando no estemos trabajando en él.
- **Cambiá tus contraseñas regularmente** y jamás las compartas con nadie, ni siquiera con los jefes. Recordemos que para que sea robusta debe contener como mínimo 8 caracteres, una mayúscula, un número y un carácter especial. Es fundamental que no utilices la misma contraseña para todos los perfiles/cuentas.
- **Activá el Múltiple Factor de Autenticación** en todos los servicios y apps que permitan esta configuración, sobre todo si tenés instaladas aplicaciones con información laboral en tu celular personal.
- Recordá que **la seguridad de tus contraseñas no solo depende de vos**, sino también del sitio donde las ingreses. Muchas veces visitamos sitios que no son seguros y las contraseñas se ven comprometidas. En este sentido, recomendamos verificar que la dirección URL del sitio al que queramos acceder esté bien escrita y que comience con HTTPS. Además, chequear que el certificado SSL del sitio esté expendido a quien corresponda, esto lo podés ver haciendo click en el candadito que aparece en la barra de navegación.

Se recomienda no anotar las contraseñas, en caso de ser muy necesario es mejor utilizar un gestor de contraseñas confiable.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

CORREO ELECTRÓNICO:

- **Prestá atención respecto a correos electrónicos fraudulentos**, es decir campañas de phishing. A través de estos podríamos infectar el equipo con un malware o generar una fuga de información. Recordá no hacer click en enlaces ni descargar archivos adjuntos que provengan de un remitente desconocido o sospechoso.
- **Utilizá el mail institucional**, sobre todo para realizar intercambio de archivos oficiales. Si no poseés una cuenta, recomendamos que la solicites cuanto antes al sector correspondiente.

EN UN MUNDO CADA VEZ MÁS HIPERCONECTADO, ES MUY IMPORTANTE TENER PRESENTE QUE LA SEGURIDAD DIGITAL ES UN ASUNTO DE TODOS POR IGUAL Y EMPIEZA POR CADA UNO DE NOSOTROS.

SEGURIDAD DE LA INFORMACIÓN:

- Siempre que sea posible **trabajá los archivos desde la Nube**, es decir, no los descargues localmente a tu dispositivo para editarlos. La mayoría de los servicios de este tipo cuentan con editores online.
- Asegurate de **sincronizar bien todos los archivos** para así evitar pérdidas de información.
- **No almacenes información sensible y/o confidencial en pendrives** o discos extraíbles personales.
- Si necesitás **compartir un archivo o documento confidencial podés encriptarlo** para enviarlo por correo electrónico y hacerle llegar al destinatario la contraseña por otro medio o plataforma.

SEGURIDAD EN LOS NAVEGADORES WEB:

- **Mantené actualizado el navegador web** que se utilice **y sus plugins** o extenciones.
- **Eliminá todos los plugins que desconozcas** o que no sepas para qué sirven ya que podrían tratarse de algún tipo de malware.
- **Prestá atención a los gestores de contraseñas** que vienen instalados por defecto en los navegadores para que no guarden datos de inicio de sesión.

¿QUÉ ES EL PHISHING?

El “phishing” es una práctica de ingeniería social que tiene como objetivo apropiarse de datos personales ajenos para usarlos en beneficio propio.

+ INFO

La información más buscada a través de ésta técnica son credenciales de acceso a mails y otros servicios online, claves de cuentas bancarias y datos de tarjetas de crédito.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

EN CASO DE ESTAR UTILIZANDO DISPOSITIVOS ELECTRÓNICOS PERSONALES

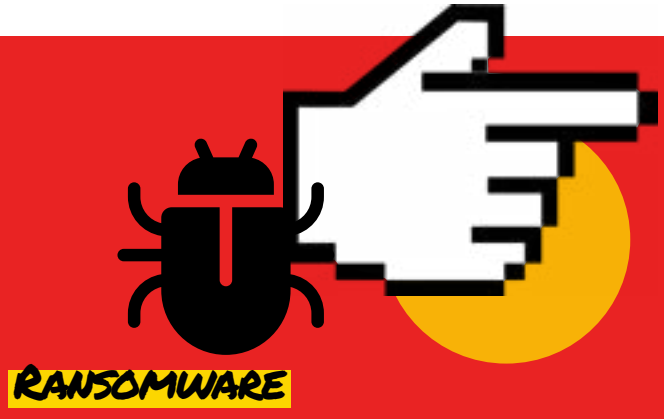
Si no contamos con la posibilidad de que nuestro empleador nos brinde una notebook y para cumplir nuestras funciones laborales tenemos que utilizar nuestros propios dispositivos, **hay una serie de medidas que debemos tener muy en cuenta además de las ya mencionadas**, sobre todo si se trata de dispositivos de uso compartido.

- Creá un usuario con contraseña destinado específicamente para trabajar.
- Jamás utilizar una computadora o notebook de uso público.
- Tené la precaución de borrar correctamente datos y documentación confidencial de las carpetas que hayas utilizado y de la papelera de reciclaje.
- Asegurate de que el sistema operativo se encuentra totalmente actualizado, como así también el programa antivirus que tengas instalado.
- Si se trata de un dispositivo móvil (celular o tablet), descargá las aplicaciones que necesites únicamente de las tiendas oficiales de Android o iOS.
- Evitá mezclar tu vida privada con la laboral, esto quiere decir que mientras estés trabajando evites usar tus redes sociales, correo electrónico personal y homebanking (o similares) al mismo tiempo.
- Si sentís que tu dispositivo personal no es seguro para trabajar con información sensible, informales a tus superiores de esta situación para poder solucionarla como crean conveniente.

¿QUÉ ES UN RANSOMWARE?

Es un malware que afecta a los sistemas encriptando y denegando el acceso a la información a los usuarios. Por medio de una extorsión exige el pago de un rescate para eliminar dicha restricción. Es consideraro un delito.

MALWARE (DEL INGLÉS “MALICIOUS SOFTWARE”) ES UN PROGRAMA MALICIOSO CUYO OBJETIVO ES ALTERAR EL FUNCIONAMIENTO NORMAL DE LOS DISPOSITIVOS ELECTRÓNICOS.



¿QUÉ HACER FRENTE A UNA INFECCIÓN POR RANSOMWARE?

Apagar inmediatamente el equipo y comunicarse cuanto antes con quién corresponda. Lo principal y fundamental es no infectar la red y los servidores. Cuanto más rápido se actúe, más posibilidades hay de limitar los daños.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

RECOMENDACIONES PARA LAS INSTITUCIONES, EMPRESAS Y PYMES

Desde BA-CSIRT recomendamos, en la medida de lo posible, que los empleadores equipen a sus empleados con dispositivos que cumplan con las políticas de seguridad de la información correspondientes a cada institución.

Si esto no es posible y el usuario deberá utilizar sus dispositivos personales para poder desarrollar sus tareas laborales, lo ideal sería que, en conjunto con el área de sistemas, IT o quien corresponda, verifiquen que dichos dispositivos se encuentren en las correctas condiciones de seguridad: sistema operativo y antivirus actualizados.

Por otra parte, queremos destacar la importancia de **capacitar a todas las personas que forman parte de las instituciones/empresas en materia de ciberseguridad** ya que estas acciones **pueden reducir hasta en un 90% las probabilidades de sufrir un ataque** a nivel corporativo o institucional.

DADA LA ALTA EXPOSICIÓN QUE SE TIENE A LOS VIRUS INFORMÁTICOS, ES IMPRESCINDIBLE HACER USO DE PROGRAMAS ANTIVIRUS EN TODOS LOS DISPOSITIVOS QUE SE UTILICEN CONECTADOS A INTERNET.

¿PARA QUÉ SIRVE UNA VPN?

Permite crear una red local sin necesidad de que sus integrantes estén físicamente conectados entre sí, sino a través de Internet. Idealmente la conexión está cifrada, de esta manera nadie podrá saber a qué se está accediendo.

VPN son las siglas de Virtual Private Network, o Red Privada Virtual.

RECOMENDACIONES GENERALES:

CONECTIVIDAD:

- **Utilizar una conexión VPN** ya que, a través de ella, se establece una conexión remota segura (encriptada) a la red institucional.
- En caso de no disponer de una VPN, **no es recomendable utilizar una de terceros, y mucho menos si es gratuita** ya que se podría estar filtrando información confidencial.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

CONTRASEÑAS Y CONFIGURACIONES DE SEGURIDAD:

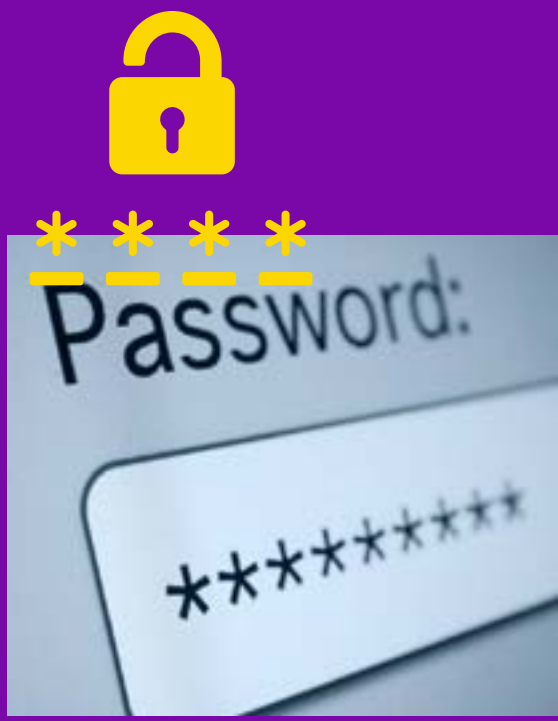
- **Definir políticas claras** que establezcan qué se permite y qué se prohíbe hacer con los dispositivos, sistemas y aplicaciones corporativas o institucionales durante el período de trabajo desde la casa.
- **Configurar el equipo para que pida una contraseña** o dato biométrico al acceder al perfil del usuario y establecer el bloqueo del dispositivo según el tiempo de inactividad.
- **Evitar instalar programas/software con licencias corporativas en equipos personales**. De ser posible, es recomendable instalarlos en equipos institucionales y que luego el usuario acceda a ellos a través de escritorio remoto por VPN.
- Siempre que sea posible, i**mplementar medidas de seguridad como Múltiple Factor de Autenticación** tanto en el correo institucional como en las plataformas y aplicaciones que se utilicen para trabajar.
- **Verificar los accesos a sistema o plataformas según el rol** que posea cada trabajador.

CORREO ELECTRÓNICO:

- **Incentivar la utilización del correo institucional** para el intercambio de archivos. Además, es fundamental hacer hincapié en que los temas oficiales deben ser tratados por canales oficiales.
- **Solicitarles a los empleados la implementación del Múltiple Factor de Autenticación app de correo** sobre todo si la tienen instalada en el celular.

SEGURIDAD DE LA INFORMACIÓN:

- **Reforzar la política de respaldo de la información** sincronizando todos los archivos en la Nube. Además, incentivar a los empleados a editar archivos desde los editores online que poseen estos servicios.
- **Realizar frecuentemente backups fuera de línea** para resguardar información, archivos, documentos y cualquier tipo de activo digital de posibles ataques ransomware.
- **Evaluar la encriptación de discos en equipos institucionales** por si estos llegasen a manos equivocadas. De esta manera se asegura que no se pueda acceder a datos sensibles y/o confidenciales.
- **Revisar las políticas autoría** para evitar inconvenientes en cuanto a los derechos de propiedad intelectual de documentos desarrollados en equipos personales de los trabajadores.
- **Digitalizar todos los documentos** que aún estén en papel y que se requieran para trabajar remotamente. Si se trata de información sensible o confidencial se recomienda configurar el bloqueo por contraseña para poder visualizarlo.



Las contraseñas deben ser: personales, secretas, intransferibles y modificables sólo por el titular.

UTILIZAR CONTRASEÑAS SEGURAS CONSTITUYE LA PRIMERA LÍNEA DE DEFENSA PARA LA PROTECCIÓN DE LA INFORMACIÓN.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

COMUNICACIÓN:

- Recomendamos **establecer canales de comunicación oficiales y ágiles** con el área de soporte para la resolución de problemas técnicos que puedan llegar a tener los usuarios.
- Implementar una **plataforma de videollamadas segura y confiable** para poder realizar reuniones no presenciales.
- Asegurarse de **capacitar y concientizar a todos los empleados** que realicen home office **sobre los riesgos relacionados a la seguridad de la información:** phishing, infección por malware, brechas de seguridad, fuga de información, etc. Como así también fomentar e incentivar las buenas prácticas de seguridad informática.

GESTIÓN DE INCIDENTES:

- **Habilitar un canal de comunicación para emergencias:** si un trabajador llega a detectar un incidente de ciberseguridad durante su jornada laboral en casa es fundamental poder actuar cuanto antes para mitigar los posibles daños.
- **Tener procedimientos claros** para actuar ante diferentes escenarios e incidentes y asegurarse que cada una de las personas que intervengan en dicho procedimiento lo sepan a la perfección.

¿QUÉ ES UN BACKUP?

Es un proceso mediante el cual se copian archivos de un lado a otro, con el objetivo de asegurar la información y teneral disponible en caso de que el lugar de guardado original se dañe, pierda o infecte con un malware.

ES FUNDAMENTAL ENTENDER QUE LAS COPIAS DE SEGURIDAD DE LA INFORMACIÓN ES LO ÚNICO REALMENTE EFECTIVO ANTE ALGÚN DAÑO O PÉRDIDA DE DATOS.

SI TUVISTE ALGÚN INCIDENTE DE CIBERSEGURIDAD NO DUDES EN COMUNICARTE CON BA-CSIRT

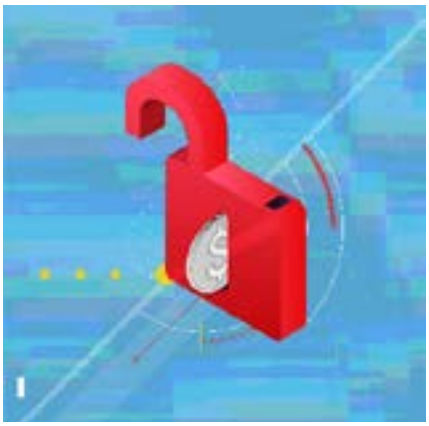
Llamanos al (011) 4323-9362 o bien escribinos a ciberseguridad@ba-csirt.gob.ar

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

MATERIALES DIDÁCTICOS A TENER EN CUENTA

En los siguientes links podrás encontrar más información específica en nuestra web sobre algunos temas que desarrollamos a lo largo de este material:

RANSOMWARE



BACKUPS

CONTRASEÑAS SEGURAS

MÚLTIPLE FACTOR DE AUTENTICACIÓN

KEYLOGGER

SEGURIDAD EN CELULARES

FUENTES

- https://www.csirt.gob.cl/media/2020/03/Protocolo-de-seguridad.pdf
- https://www.welivesecurity.com/la-es/2020/03/16/recomendaciones-seguridad-teletrabajo-covid-19/
- https://espacionegocios.com.ar/6-medidas-de-seguridad-home-office-15233/
- https://www.facebook.com/OEAoficial/videos/2924929580883612/
- https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene