COMUNICACIONES

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

Guía de Ciberseguridad

para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo

Junio de 2020

COMUNICACIONES

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

Guía de ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo

AMENAZAS MÁS COMUNES

- Códigos maliciosos o malware (virus, gusanos, troyanos, etc).
- Amenazas relacionadas con la ingeniería social utilizadas para engañar a las personas para que revelen información confidencial y descarguen o ejecuten contenido malicioso.
  - **Phishing:** ataque a través del correo electrónico.
  - **Smishing:** ataque por medio de mensajes de texto corto (SMS).
  - **Vishing:** estafa mediante llamada telefónica.

RECOMENDACIONES GENERALES

- No dejar a la vista información personal o de trabajo.
- Mantener la computadora, tableta, teléfono, celular u otro dispositivo, en un lugar seguro y con contraseña.
- Bloquear la sesión al alejarse de los dispositivos de trabajo.
- Mantener cubierta la cámara web cuando no se esté utilizando
- Deshabilitar la auto ejecución de memorias USB.
- Evitar manipular, modificar configuraciones, o prestar dispositivos proporcionados por la organización en la que trabajas.

El aumento del Teletrabajo representa un entorno propicio para los cibercriminales y muchos trabajadores se encuentran expuestos a riesgos de ciberseguridad

Recuerda que:
"Teletrabajo improvisado, ciberataque asegurado"

TELETRABAJO SEGURO UTILIZANDO DISPOSITIVOS PERSONALES

- **Sistema operativo:** Mantener actualizados los sistemas operativos y las aplicaciones de computadoras, teléfonos y tabletas.
- **Antivirus:** Instalar y mantener actualizados los antivirus.
- **Seguridad de la red Wi-Fi :** Asegurar que la red Wi-Fi cuente con contraseña y evitar la conexión a redes Wi-Fi públicas.
- **Contraseñas:** Al generar las contraseñas, éstas deben ser largas y únicas para cada dispositivo o cuenta. No las compartas con nadie.
- **Ataques con técnicas de inteligencia social:** Estar alertas a llamadas, correos, mensajes SMS y de WhatsApp, enlaces de teleconferencias e invitaciones de de remitentes desconocidos.
- **Navegación segura:** Ingresar a sitios web confiables y de preferencia teclear la dirección del sitio. Cerrar la sesión al finalizar.
- **Uso seguro de la nube:** Conocer las condiciones de uso y las políticas de privacidad del servicio a utilizar. Cerrar la sesión de la nube al concluir su uso.
- **Teleconferencias:** Descargar, instalar y actualizar la aplicación desde la página web oficial del desarrollador o desde las tiendas oficiales de apps.
- **Red Privada Virtual (VPN):** Las VPN añaden una capa extra de seguridad a tus comunicaciones,

Contenido

Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo

Introducción

Ante la emergencia sanitaria generada por el virus SARS-CoV2 y la enfermedad que éste provoca (COVID-19), **instituciones públicas y privadas están aplicando estrategias de teletrabajo**, con el fin de prevenir la propagación del virus, procurar la salud de sus colaboradores y, al mismo tiempo, mantener sus operaciones.

Si bien es cierto que esta modalidad de trabajo se ha incrementado en los últimos años, es a partir de la emergencia sanitaria que su adopción se ha acelerado.

En este contexto, **expertos en ciberseguridad advierten un entorno propicio para que prosperen los cibercriminales** y que, tanto individuos como empresas, se encuentren mayormente expuestos a múltiples amenazas de ciberseguridad[1].

¿Por qué?

- En muchas ocasiones, los **trabajadores no cuentan con la suficiente sensibilización sobre su exposición al riesgo**, o bien, no están familiarizados con las herramientas y/o capacitación de sus organizaciones para prevenir y enfrentar amenazas de ciberseguridad.

- Los **empleados** que ahora trabajan lejos de sus oficinas a menudo **utilizan redes Wi-Fi menos seguras y aprovechan dispositivos propios** que, comúnmente, no están alineados o configurados con los controles de políticas de seguridad de sus empresas, lo cual los vuelve excepcionalmente vulnerables a ataques cibernéticos.

- Los piratas informáticos eligen como blanco la **dependencia, cada vez mayor, de las personas con respecto a las herramientas digitales**, además de que más tiempo en línea incrementa la

[1] Unión Internacional de Telecomunicaciones (UIT). COVID 19: *Strategies to Reduce Cyber Risk While Working from Home (OPINION).* https://news.itu.int/covid-19-strategies-to-reduce-cyber-risk-while-working-from-home-opinion/

potencial exposición de los trabajadores a amenazas de ciberseguridad.

- Los **piratas informáticos** son **extremadamente creativos al idear formas de aprovecharse de los usuarios** y de la tecnología para acceder a contraseñas, redes y datos, a menudo sirviéndose de herramientas de ingeniería social y de temas y tendencias populares para tentar a los usuarios a tener comportamientos inseguros en línea.

En ese sentido, los **piratas informáticos están aprovechando el miedo y la confusión por la emergencia sanitaria por COVID-19** para difundir virus informáticos y/o llevar a cabo fraudes en línea, tanto a individuos como a empresas[2].

Todo lo anterior, ha creado una **enorme superficie de exposición a ataques cibernéticos** dirigidos a los empleados, la red, la computadora portátil, el teléfono inteligente, la tableta, etc. con la intención de cometer delitos informáticos.

Por ello, la Subsecretaría de Comunicaciones de la Secretaría de Comunicaciones y Transportes (SCT) ha elaborado esta **Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo**, **que contiene recomendaciones sencillas y prácticas para fomentar una buena higiene cibernética de los dispositivos utilizados para el teletrabajo y promover la ciberseguridad de las personas y de sus organizaciones**.

Amenazas más comunes a la Ciberseguridad

Una de las principales amenazas para los dispositivos tecnológicos utilizados para el teletrabajo es el ***malware***, también conocido como **código malicioso**. Éste se define como cualquier programa informático que se coloca de forma oculta en un dispositivo, con la intención de

[2] Foro Económico Mundial (WEF, por sus siglas en inglés). ¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus? https://es.weforum.org/agenda/2020/03/por-que-la-ciberseguridad-es-mas-importante-que-nunca-durante-la-pandemia-de-coronavirus/

comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo.

Los **tipos más comunes de amenazas de *malware*** incluyen virus, gusanos, troyanos, *rootkits*[3] y *spyware*[4]. Las amenazas de *malware* pueden infectar cualquier dispositivo por medio del correo electrónico, los sitios web, las descargas y el uso compartido de archivos, el software punto a punto y la mensajería instantánea[5].

Además, **existen amenazas relacionadas con la ingeniería social como el *Phishing, Smishing y Vishing***[6], por medio de las cuales los atacantes intentan engañar a las personas para que revelen información confidencial o realicen ciertas acciones, como descargar y ejecutar archivos que parecen ser benignos, pero que en realidad son maliciosos:

- El ***Phishing*** es un método de ataque a través del correo electrónico enviado por un delincuente pretendiendo ser otra persona, compañía o sitio de confianza, para robar la contraseña o información sensible. Este tipo de amenazas también pueden buscar tomar el control del dispositivo o computadora.

- El ***Smishing*** ocurre cuando se recibe un mensaje de texto corto (SMS) al teléfono celular, por medio del cual se solicita al usuario llamar a un número de teléfono o ir a un sitio web.

- El ***Vishing*** es la estafa que se produce mediante una llamada telefónica que busca engañar, suplantando la identidad de una

[3] Karspersky. *¿Qué es un Rootkit?: Es un tipo de malware diseñado para infectar una PC, el cual permite instalar diferentes herramientas que dan acceso remoto al ordenador. Este malware se oculta en la máquina, dentro del sistema operativo y sortea obstáculos como aplicaciones antimalware o algunos productos de seguridad. El rootkit contiene diferentes herramientas maliciosas como un módulo para robar los números de tarjeta o cuentas bancarias, un bot para ataques y otras funciones que pueden desactivar el software de seguridad.* https://www.kaspersky.es/blog/que-es-un-rootkit/594/.

[4] Avast. *Spyware: detección, prevención y eliminación. El Spyware es un tipo de malware que puede rastrear y registrar la actividad en equipos y dispositivos móviles. Hay cepas con comportamientos específicos; en general, los ciberladrones usan el spyware para recabar datos e información personal.* https://www.avast.com/es-es/c-spyware

[5] *Scarfone y Souppaya. "User's Guide to Securing External Devices for Telework and Remote Access Recommendations of the National Institute of Standards and Technology" 2016. National Institute of Standards and Technology (NIST).* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-114.pdf

[6] Santander. Cómo detectar el *phishing*. https://www.santander.com/es/stories/como-detectar-el-phishing

persona o entidad para solicitar información privada o realizar alguna acción en contra de la víctima.

Recomendaciones de Ciberseguridad

En la actualidad existen muchas **herramientas para minimizar los riesgos y amenazas** de ciberseguridad derivados de la mayor exposición de las personas por el **aumento del teletrabajo**.

Recomendaciones generales

- **No dejar a la vista de otras personas información relevante,** como aquélla sensible o claves de acceso, ni documentos o carpetas de trabajo.

- **Mantener** siempre la **computadora, tableta, teléfono celular** o cualquier otro dispositivo para el trabajo, **en un lugar seguro y con contraseña**, a fin de restringir el acceso de personas no autorizadas.

- **Al alejarse** de los dispositivos de trabajo, es importante **bloquear la sesión**.

- Mantener **cubierta la cámara web cuando no se esté utilizando**, para limitar el acceso que pudieran llegar a tener a ésta aplicaciones o programas no autorizados.

- **Deshabilitar la auto ejecución de memorias USB**, para evitar que, por ese medio, se instalen programas maliciosos.

- Si tu organización facilita los recursos necesarios para el teletrabajo, es indispensable **realizar un uso exclusivamente profesional de los medios proporcionados**. No se recomienda, en ninguna circunstancia, manipularlos, modificar su configuración, o prestarlos a otras personas.

- **Realizar copias de seguridad periódicas de la información** para garantizar el acceso a la información almacenada, ya sea personal o de la organización. Así, en caso de que ocurra cualquier incidente de

seguridad(robo, pérdida del dispositivo, o avería, etc.), se podrá mantener el acceso a la misma.

- **Proteger con contraseña (encriptar) los dispositivos** donde se almacene información (memorias USB o discos externos) para proteger la información de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

Recomendaciones para trabajar a distancia de manera segura utilizando los dispositivos personales

En caso de que los empleados utilicen dispositivos personales para el teletrabajo (política conocida como *BYOD o Bring Your Own Device*), aunque éstos no cuenten con las mismas políticas de seguridad que los institucionales, los trabajadores pueden reducir sus vulnerabilidades poniendo en práctica las siguientes recomendaciones:

Sistema Operativo

- **Mantener actualizados los sistemas operativos y las aplicaciones** de los dispositivos, incluidas las computadoras personales (PC), los teléfonos inteligentes y las tabletas. Estas actualizaciones incluyen cambios importantes que mejoran el rendimiento y la seguridad de los equipos; muchos de estos programas, incluso, se actualizan de manera automática.

- Se recomienda **activar funcionalidades de protección, como el cortafuegos (*firewall*), incorporadas en los sistemas operativos más comunes**. Un cortafuegos es la primera línea de defensa ante un ataque a tu red desde Internet y permite proteger el equipo de programas maliciosos o de atacantes que intenten conectarse al equipo de forma remota[7]. Además, permite establecer reglas para indicar qué conexiones de red se deben aceptar y cuáles no. Al

[7] **Soporte de** Microsoft. Activar o desactivar el Firewall de Microsoft Defender**.**
https://support.microsoft.com/es-es/help/4028544/windows-10-turn-microsoft-defender-firewall-on-or-off

mismo tiempo, admite el normal intercambio de datos entre la computadora y servicios verificados de Internet.

Antivirus

Los antivirus son programas que ayudan a proteger los dispositivos contra la mayoría de los virus, gusanos, troyanos y otros tipos de *malware* que pueden infectar a los dispositivos, por ello se recomienda:

- Instalar y mantener actualizados los **antivirus, prefiriendo aquéllos** que incorporan funcionalidades de protección contra *malware* y cortafuegos (*firewall*), también conocidos como **"*suites* de seguridad"** .

- **Evitar tener dos antivirus en un mismo dispositivo. Tener dos antivirus activos no significa mayor protección**; de hecho, puede ocasionar diferentes problemas en el sistema. Un antivirus que esté trabajando se convertirá en un "software malicioso" a los ojos del otro, el cual intentará bloquearlo y eliminarlo, y se corre el riesgo de afectar el desempeño del sistema por el consumo extra de recursos[8].

- **Todas las instalaciones y actualizaciones de programas y aplicaciones deben hacerse desde el sitio web oficial del fabricante**[9] **o desde las tiendas oficiales de apps** -verificando la identidad del autor de la aplicación-, evitando descargar e instalar aquéllas de dudosa procedencia.

Seguridad de la red Wi-Fi

Una parte importante del teletrabajo es la **aplicación de medidas de seguridad de las redes en el hogar**. Es cada vez más común que los usuarios cuenten en casa con un ruteador inalámbrico (Wi-Fi) para conectar sus dispositivos a Internet sin necesidad de cables.

[8] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). ¿Sabías que utilizar tus dispositivos personales para trabajar puede ser peligroso? https://www.osi.es/es/actualidad/blog/2019/05/15/sabias-que-utilizar-tus-dispositivos-personales-para-trabajar-puede-ser
[9] Ídem.

Para evitar que usuarios no autorizados se conecten de forma inalámbrica al ruteador y tengan la posibilidad de acceder a la conexión, e incluso al resto de los dispositivos conectados y a la información que se transmite, **es importante asegurar que la red Wi-Fi cuente con contraseña que el usuario debe introducir al conectar por primera vez un dispositivo.**

Los ruteadores ofrecen varios tipos de contraseñas y cifrados (**que codifican los datos del usuario, usando un valor o clave secreta** y los hace incomprensibles para terceros), como los siguientes:

- **Las redes sin cifrado, o abiertas**, son aquéllas que no tienen ninguna contraseña o cifrado y permiten a cualquier usuario conectarse. Una red con estas características **no es recomendable**.

- El **cifrado *Wired Equivalent Privacy*** (WEP, por sus siglas en inglés) es considerado, hoy en día, un **sistema poco seguro y no se aconseja su utilización** ya que, con las herramientas y conocimientos adecuados, se puede llegar a conseguir la clave de acceso a la red Wi-Fi en pocos minutos.

- El **cifrado *Wi-Fi Protected Access*** (WPA, por sus siglas en inglés), específicamente en su versión 2 (WPA2) o más actualizada, **es considerado seguro y se recomienda comprobar que esté habilitado** como parte de las medidas de seguridad de la red.

  Para comprobarlo, es necesario entrar desde la computadora a las propiedades de la red, para ver el tipo de seguridad de la conexión. **Se recomienda tener habilitada alguna de las variantes de WPA2**, al menos[10]. Puedes solicitar apoyo a tu proveedor de servicios de Internet para más orientación.

- Se recomienda **cambiar las contraseñas predeterminadas en el ruteador por unas de elección del usuario, utilizando una contraseña robusta para la red Wi-Fi**. Asimismo, se recomienda que incluya mayúsculas, minúsculas, números y símbolos. Cuanto

[10] Santander. Redes más seguras en casa. https://www.santander.com/es/stories/redes-mas-seguras-en-casa

mayor sea la longitud de la contraseña, más difícil será que un atacante pueda descubrirla[11].

- Es **importante evitar compartir la clave de la red Wi-Fi con otras personas**, pues quien tenga acceso a tu red inalámbrica podría tener acceso a todos los dispositivos conectados a ella.

- Es importante **evitar la conexión a redes Wi-Fi públicas abiertas** (o *hotspots* Wi-Fi). Estas redes son totalmente inseguras ya que permiten que cualquier dispositivo se conecte al ruteador sin ningún tipo de seguridad, por lo que cualquier usuario podría capturar la información se transmita a través de dicha conexión.

Contraseñas

Las **contraseñas protegen la información que contienen los dispositivos y cuentas de los usuarios**. No obstante, ante la cantidad de claves y combinaciones que cotidianamente se deben utilizar, la mayoría de las personas opta por contraseñas fáciles de recordar por la comodidad que esto implica, o bien, por la falta de conocimiento de lo fácil que puede ser para un ciberdelincuente obtenerlas.

Para asegurar la efectividad de las contraseñas y evitar el robo de éstas, es recomendable poner en práctica las siguientes acciones[12]:

- **Al generar las contraseñas de los dispositivos y cuentas** se deben utilizar claves largas y únicas para cada caso, **evitando utilizar la misma contraseña** para diferentes dispositivos o cuentas.

- Se deben **evitar las combinaciones sencillas** como fechas de nacimiento, secuencias consecutivas, repeticiones de un mismo dígito o palabras simples como "*password*" o "contraseña".

[11] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Tu router, tu castillo. Medidas básicas para su protección. https://www.osi.es/es/actualidad/blog/2016/11/03/tu-router-tu-castillo-medidas-basicas-para-su-proteccion
[12] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Campañas/ Contraseñas Seguras. https://www.osi.es/es/campanas/contrasenas-seguras

- La mayor **longitud de la contraseña**, así como la **incorporación de mayúsculas, minúsculas, números y caracteres especiales**, contribuyen a que ésta sea más segura y difícil de vulnerar.

- Se debe **evitar escribir contraseñas en papeles o tener archivos con esa información** que sean fácilmente accesibles para otros.

- **Habilitar el doble factor de autenticación o verificación en dos pasos**. Esta medida es una capa adicional de seguridad disponible para cada vez más servicios en la que, además de la contraseña, durante el inicio de sesión se solicita información sobre otro medio al que sólo el usuario autorizado tiene acceso (por ejemplo, verificación para entrar al correo electrónico mediante la recepción de un código vía SMS, llamada o mensaje de WhatsApp).

- Es importante **no facilitar a nadie, aunque así lo solicite, por ningún medio, contraseñas y/o códigos** para el inicio de sesión.

- Es recomendable **cambiar con frecuencia las contraseñas** a efecto de evitar accesos no autorizados.

Ataques con técnicas de inteligencia social

Los ataques de ingeniería social **buscan engañar a los usuarios para obtener nombres de usuario y contraseñas, así como otra información** sensible.

La capacidad de **identificar un ataque de ingeniería social minimiza, en gran medida, el riesgo de ser víctimas de los ciberdelincuentes** y ver comprometida información personal o de la organización para la que trabajamos. Para ello, se recomienda[13]:

- **Estar alertas ante comunicaciones**, como llamadas, correos electrónicos, mensajes cortos (SMS), enlaces de teleconferencias e invitaciones de calendario, **de remitentes desconocidos.**

[13] Santander. Cómo detectar el phishing. https://www.santander.com/es/stories/como-detectar-el-phishing

- **Antes de abrir cualquier enlace, archivo anexo, mensaje de texto o llamada** de un remitente desconocido, **hay que preguntarse** lo siguiente:

    - **¿Espero esa información?** Si el mensaje proviene de un remitente desconocido (persona u organización), **analizar bien antes de responder o hacer clic y/o descargar** cualquier archivo adjunto.
    - **¿Reconozco al remitente? Comprobar si la dirección está bien escrita** (verificar que no haga falta ninguna letra, por ejemplo) y si el dominio (la terminación del correo electrónico) **es de confianza y corresponde al nombre de quien envía el mensaje**.
    - **¿Solicitan que haga algo?** Los correos electrónicos fraudulentos (*phishing*) o los mensajes de texto de este tipo (*smishing*) **suelen pedir que se realice alguna acción** como: **hacer clic** en un hipervínculo, **descargar** algún archivo, responder al mensaje proporcionando información personal, etc. Con frecuencia, **buscan generar una sensación de urgencia y provocar una reacción inmediata e irracional**. **Es necesario analizar con calma** antes de proporcionar cualquier información que pudiera resultar comprometedora.
    - Se debe **desconfiar, particularmente, de los mensajes que parecerían genéricos** (como “Estimados:”, “A quien corresponda:”, etc.).
    - En el caso de **comunicaciones referentes a instituciones bancarias y financieras**, se recomienda **NUNCA dar clic en los enlaces contenidos en un correo o mensaje y NO proporcionar información de acceso a tus cuentas**. Si tienes alguna duda, debes contactar directamente a tu institución financiera (utilizando el número telefónico que vienen atrás de tu tarjeta, por ejemplo) para más orientación.

Navegación segura

A efecto de promover la navegación segura en Internet, se sugiere adoptar las siguientes recomendaciones:

- **Ingresar sólo a sitios web confiables**, escribiendo uno mismo la dirección de la página a la que se quiere acceder y evitando utilizar ligas proporcionadas por terceros.

- **Conocer y aplicar las funcionalidades de "navegación privada"** o **"navegación segura"**, que impiden el almacenamiento del historial en el navegador, así como imágenes, nombres de usuario y contraseñas.

- Cuando se realicen transacciones o intercambio de información sensible, **asegurarse de que la dirección de la página web comience con "https"** (no "http"), lo que contribuye a mantener segura la información transmitida.

- **Desactivar la compartición de tu ubicación geográfica**, a menos que sea estrictamente necesario.

- **Evitar el ingreso de información personal en formularios dudosos**. Si te encuentras ante un formulario que solicita información sensible (por ejemplo, nombre de usuario y contraseña), es recomendable verificar la legitimidad del sitio antes de responder.

- Al terminar de navegar en Internet, es **importante cerrar la sesión, sobre todo si se utiliza un equipo compartido**, para evitar que otras personas tengan acceso a cuentas e información privada.

Uso seguro de las herramientas de la nube

La nube permite almacenar y administrar datos, así como ejecutar aplicaciones en línea, entre muchas otras funciones. Con relación al almacenamiento, **la nube permite acceder a archivos y datos desde cualquier dispositivo conectado a Internet**; es decir, la **información está disponible en cualquier lugar en el que te encuentres y siempre que la necesites**[14].

[14] Microsoft Azure. ¿Qué es la nube? https://azure.microsoft.com/es-es/overview/what-is-the-cloud/

Para hacer uso de los servicios de la nube de manera segura y evitar el robo o mala utilización de la información almacenada, es conveniente tener en mente las siguientes recomendaciones[15]:

- Tener conocimiento de las **condiciones de uso y las políticas de privacidad** antes de utilizar cualquier servicio en la nube.

- Utilizar servicios de almacenamiento que cuenten con **cifrado "https" y certificado de seguridad.** Esto lo puedes verificar en la barra de direcciones de tu navegador de Internet.

- **No subir a la nube información sensible con acceso público o abierto**. Se recomienda utilizar herramientas de cifrado, como es el uso de **carpetas con contraseña y acceso restringido**.

- **Verificar periódicamente los archivos y carpetas que tenemos compartidos** desde nuestra cuenta, a fin de **deshabilitar los enlaces y acceso de terceros que ya no sean necesarios**.

- **Utilizar contraseñas robustas para acceder al servicio** y, preferentemente, activar el doble factor de autenticación o verificación en dos pasos.

- Realizar periódicamente un **respaldo de la información almacenada** en la nube en otro tipo de dispositivo, por ejemplo, en un disco duro externo debidamente protegido por contraseña. De esa manera, se mantiene el acceso a la información en caso de cualquier contratiempo, como una conexión limitada a Internet.

- **Cerrar la sesión de la nube al concluir las actividades** que se estén realizando.

[15] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Tu información en la nube. https://www.osi.es/es/tu-informacion-en-la-nube

Teleconferencias

La demanda de servicios de teleconferencias, especialmente a partir de la emergencia sanitaria generada por COVID-19, **se ha incrementado considerablemente**. Las teleconferencias se han convertido en una herramienta indispensable para el trabajo de muchas personas, e incluso, el medio para dar continuidad a asuntos laborales, la vida cotidiana y la comunicación con familiares y amigos.

Lo novedoso de estos servicios para muchos usuarios y la aparición de algunas vulnerabilidades en ciertas plataformas, supone para los ciberdelincuentes la **oportunidad para el acceso no autorizado** a información, robo de credenciales y acceso a los distintos recursos del dispositivo (como micrófono, cámara, etc.)[16].

Por lo anterior, es necesario **promover la adecuada protección de los usuarios** para evitar incidentes al usar estos servicios[17] tales como:

- **Informarse sobre las políticas de privacidad y las medidas de seguridad que implementa el servicio** que se desea utilizar.

- **Descargar e instalar la aplicación correspondiente desde la página web oficial del desarrollador** o **desde las tiendas oficiales** de apps.

- **Mantener actualizada la aplicación que se utilice**, pues es a través de este proceso que se puede asegurar que las vulnerabilidades detectadas y corregidas por el desarrollador se están implementando.

- Al organizar una teleconferencia se recomienda tener en cuenta:

    - En el caso de reuniones privadas, **compartir el enlace** directamente con los participantes, **haciendo uso de las**

[16] Jaimovich Desirée. (02 de abril de 2020). Zoom: alertan por graves fallas de seguridad en la popular aplicación de videollamadas. Infobae. https://www.infobae.com/america/tecno/2020/04/02/zoom-alertan-por-graves-fallas-de-seguridad-en-la-popular-aplicacion-de-videollamadas/
[17] Instituto Nacional de Ciberseguridad de España (INCIBE). Aplica estos consejos y protege tus videollamadas. https://www.incibe.es/protege-tu-empresa/blog/aplica-estos-consejos-y-protege-tus-videollamadas

funciones de compartición de las propias aplicaciones, y evitando el uso de redes sociales o canales de comunicación abiertos que podrían promover accesos no deseados.
    - **Proteger la conferencia con una contraseña robusta**, para restringir el acceso a ésta a personas no autorizadas.
    - Si la plataforma la incorpora, **activar la funcionalidad que permite al organizador verificar y, en su caso, aprobar el acceso de los participantes** que deseen acceder a la teleconferencia.

- Los participantes en teleconferencias deben **evitar compartir su escritorio de forma predeterminada** ya que esto podría provocar fugas de información.

- Se debe **cuidar el encendido del micrófono y la cámara de video** para evitar situaciones incómodas o embarazosas.

- **Si la teleconferencia es grabada, el organizador debe comunicarlo** a los participantes.

Red Privada Virtual

Una **Red Privada Virtual** (**VPN**, por su acrónimo en inglés) es un **servicio mediante el cual se establece una conexión segura a través de Internet**, entre los usuarios y los servicios o páginas web de Internet a los que éstos acceden[18].

Si imaginamos el Internet como un río en el que fluye el agua (datos e información), la VPN es un tubo, sumergido en el río, que impide ver todo lo que pasa dentro de él, debido a que la conexión entre los dispositivos y el servidor VPN siempre está cifrada (protegida). De esa manera, **si alguien interceptara tus comunicaciones, sería incapaz de interpretar la información transmitida**.

En algunas ocasiones, **las empresas ponen a disposición de sus empleados acceso a través de VPN**; **de no ser éste el caso** o para añadir

[18] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Te explicamos qué es una VPN y para qué se usa. https://www.osi.es/es/actualidad/blog/2016/11/08/te-explicamos-que-es-una-vpn-y-para-que-se-usa

una capa extra de seguridad a tus comunicaciones personales, **las VPN pueden contratarse como servicio** (**no se recomienda utilizar servicios de VPN gratuitos**, pues éstos podrían tener el efecto contrario al deseado de proteger la información). En este sentido, es esencial **utilizar un servidor VPN de confianza para el teletrabajo**.

Recursos

A continuación, se ponen a disposición algunos **recursos de interés**, que pudieran resultar de utilidad para quienes participan en el teletrabajo:

- Simulador de Ciberseguridad de la SCT.
- Cursos en línea y certificaciones través de los Centros de Inclusión Digital de la SCT, en colaboración con Coursera.
- Plan de aprendizaje en Ciberseguridad de Open P-TECH.
- Recurso pedagógico para mejorar contraseñas del Instituto Nacional de Ciberseguridad de España (INCIBE).
- Recomendaciones al elegir una suite de seguridad de la Coordinación de Seguridad de la Información de la UNAM (UNAM CERT).
- Plataformas de videoconferencia y aspectos de seguridad que te interesa conocer del INCIBE.

Conclusión

El teletrabajo abre nuevas posibilidades y, a la vez, nuevas vulnerabilidades de las que debemos estar conscientes y alertas para responder de manera adecuada.

El acceso a Internet está cada día más presente en la vida de las personas y, en ese sentido, el uso seguro de las telecomunicaciones en apoyo a teletrabajo cobra especial relevancia como un quehacer que nos atañe a todos quienes usamos estos servicios.

Tomando en consideración que expertos advierten que “teletrabajo improvisado, ciberataque asegurado”, es importante continuar el desarrollo de instrumentos que, como esta guía, contribuyan a seguir avanzando en el impulso del uso seguro de las telecomunicaciones en apoyo al teletrabajo, en beneficio de todas y todos los mexicanos.