Medidas de seguridad para acceso remoto (teletrabajo)

En la actualidad, existen múltiples campañas de phishing y ransomware activas y dado que las situaciones que conllevan a la utilización de conexiones remotas pueden ser una vía de entrada de ingeniería social y código dañino a los sistemas, se considera clave poder garantizar la seguridad de los sistemas de información y de estas conexiones y accesos.

Una vez que equipos portátiles, smartphones o tabletas se llevan fuera de la infraestructura de red de una entidad y se conecten a nuevas redes y wifi, los riesgos se amplían y aumentan. Debemos extremar las precauciones cuando estamos fuera de nuestro entorno habitual de trabajo, protegiendo nuestros dispositivos con diferentes herramientas que aumenten su seguridad, los datos que contienen y las comunicaciones que hagamos con ellos.

"*El Coronavirus no solo está poniendo en jaque la salud de las personas, ya que también está siendo utilizado como cebo por los ciberdelincuentes para propagar malware. Además de un aumento en el trabajo remoto para proteger la salud de los trabajadores, hemos visto cómo delincuentes informáticos intentan aprovechar el interés que ha causado el virus, ocultando archivos maliciosos en documentos que supuestamente se relacionan con la enfermedad, por lo que a medida que las personas continúen preocupadas sobre el brote, es posible que veamos más y más malware oculto en archivos falsos que contienen una variedad de amenazas, desde troyanos hasta gusanos que son capaces de destruir, bloquear, modificar o copiar datos, así como interferir en el correcto funcionamiento de las computadoras"*.*

La seguridad se concibe como un conjunto de medidas que son implementadas para disminuir el riesgo, aumentar la protección y garantizar el bienestar de los objetos o individuos. En la modalidad de teletrabajo se debe velar por garantizar la seguridad de la información, tanto de los equipos como de los teletrabajadores. Estos últimos trasladan numerosos datos y contenidos a dispositivos electrónicos con nuevas ubicaciones físicas generando nuevos riesgos que se deben mitigar estableciendo protocolos adecuados. Tales políticas de seguridad se establecen como planes de acción encargados de afrontar, mitigar y prevenir los riesgos originados con la implementación del teletrabajo.

Por lo tanto, el objeto del presente documento es garantizar esta seguridad desde los lugares de teletrabajo:

- **Confidencialidad**: asegurar el acceso a la información únicamente por las personas autorizadas, que son los teletrabajadores.
- **Integridad**: mantener los datos libres de modificaciones no autorizadas.
- **Disponibilidad**: garantizar que la información esté en disposición para los teletrabajadores en cualquier momento, de tal forma que puedan desarrollar sus actividades.
- **Autenticación**: identificar al usuario generador de la información.

Medidas de seguridad para acceso remoto (teletrabajo)

Existen dos soluciones para la implementación de un sistema de acceso remoto seguro en función de las capacidades de la organización:

- De un lado, la solución basada en la **nube** que permite un despliegue rápido de una solución de acceso remoto seguro, aunque no se disponga de una gran capacidad dentro de la organización.
- De otra, una solución basada en **sistemas locales**, on-premise, en la que se extienden los límites de la organización más allá de sus instalaciones. En este caso, se despliegan portátiles configurados y bastionados para que puedan utilizar Internet como medio de acceso para acceder de forma segura a los servicios corporativos.

Cada organización es responsable de conocer y evaluar los factores que le son de aplicación previamente al diseño o replanteo del sistema, la reserva de recursos y la selección de componentes a incluir.

Por ejemplo, en el caso de **Alaro Avant**, el acceso a la información se realizará desde el domicilio del trabajador o, en su caso, desde entornos particulares del trabajador, a través de la conexión a la VPN instalada en los equipos portátiles facilitados por la entidad a sus trabajadores. La conexión a la VPN debe realizarse desde redes wifi privadas o utilizando conexiones 4G/5G compartidas de los móviles, por lo que queda prohibido el uso de redes wifi públicas (hoteles, cafeterías, aeropuertos, etc.).

Correo electrónico

Si se plantea un escenario en el que los usuarios puedan acceder al sistema de correo electrónico corporativo desde equipos informáticos no gestionados por la organización a través de Internet, se recomienda reforzar la inspección de los correos electrónicos antes de ser entregados a los usuarios.

En este caso, pueden aumentarse las probabilidades de ser víctimas de ataques al poder tener implementadas medidas menos seguras en los ordenadores remotos y que en la organización se detectarían y tratarían al tener controlado el perímetro de seguridad, aspecto que en los equipos remotos no se puede garantizar.

Es importante controlar los motores de antivirus e inspección de los buzones de correo electrónico hacia atrás en el tiempo de las personas que tengan tanto acceso remoto como acceso al correo electrónico corporativo.

No se deberán utilizar datos sensibles de la organización o información que legalmente deba ser protegida en equipos que no pertenezcan a la organización.

Si los miembros de una organización deben enviarse correos internos, pero ya no se puede utilizar la red interna es conveniente usar mecanismos de cifrado, como PGP (Pretty Good Privacy), para el cifrado de los correos y así mantener la confidencialidad y no repudio.

Reuniones virtuales

Si se plantea un escenario en el que los usuarios puedan acceder a salas de reuniones/conferencias de forma virtual o telemática desde equipos informáticos no gestionados por la organización a través de Internet, se debería revisar la seguridad o haberse aplicado los parches de seguridad correspondientes.

Además, se debe tener un listado de servicios acordados para mantener reuniones de forma virtual, conocer las licencias de las que se disponen o si se van a utilizar herramientas gratuitas.

En todos los casos conviene tener controlados los accesos a la red y sistemas de la entidad, además de tener la posibilidad en los dispositivos perimetrales de habilitar reglas con fecha y hora de inicio y finalización.

Cuando se inicien reuniones por medio de estos canales, se debe revisar que los asistentes son los invitados y no se tienen duplicados, personas no invitadas o desconocidas en la reunión.

Se debe revisar si la reunión es grabada, que quede registro de las personas conectadas, donde se almacena y que personas pueden grabar la reunión dentro de la misma.

Por ejemplo, en el caso de **Alaro Avant**, los trabajadores únicamente podrán utilizar las herramientas instaladas por su proveedor de servicio técnico en los equipos portátiles. En caso de necesitar instalar una nueva aplicación, los trabajadores deberán realizar la petición al proveedor del servicio técnico.

Personas o equipos con acceso remoto

Los trabajadores deben disponer, de forma diaria, de los portátiles o equipos facilitados por la entidad para acceder remotamente a los sistemas de información de la misma.

En estas situaciones conviene realizar pruebas de conectividad de los diferentes usuarios que pudieran utilizar el acceso remoto comprobando su funcionalidad y registrando las direcciones IP de acceso remoto, credenciales y accesos disponibles mediante la conexión remota.

En todo acceso remoto, es importante asegurar las siguientes medidas:

- Tener actualizado el puesto de trabajo con los últimos parches de seguridad (sistema operativo, herramientas de seguridad, aplicaciones, etc.).
- Cerrar todas las conexiones que no sean estrictamente necesarias.
- Cerrar todas las aplicaciones cuando no se estén utilizando.
- Desconectar el equipo de internet cuando no se necesite
- Realizar análisis programado de los antivirus (exhaustivos) a los puestos de trabajo, aunque los ordenadores no se reinicien.
- Aplicar las actualizaciones programadas en la organización, para ello puede ser necesario apagar y encender los equipos de forma periódica.
- Prever mecanismos que permitan el reinicio de estas máquinas de forma remota y acceder por canales establecidos a las mismas desde fuera de la organización una vez se reiniciara el equipo.
- No abrir enlaces y descargar archivos de dudosa procedencia o responder a mensajes no solicitados.

Se recomienda tener un listado de las direcciones IP de los posibles orígenes remotos de las conexiones.

Por ejemplo, en el caso de **Alaro Avant**, los trabajadores únicamente utilizarán los equipos portátiles proporcionados por la entidad para la conexión VPN al servidor de ficheros. En caso de necesitar instalar una nueva aplicación, los trabajadores deberán realizar la petición al proveedor

del servicio técnico. Los trabajadores deberán apagar su equipo al finalizar la jornada laboral, de forma que puedan realizarse las actualizaciones correspondientes; y deberán comunicar al proveedor del servicio técnico, cualquier incidencia que pueda poner en peligro la seguridad de la información de la entidad.

Recomendaciones para un teletrabajo seguro

- No regalar los datos personales a la primera de cambio. Proteger el portátil y el móvil con credenciales de acceso y diferenciar las cuentas personales de las profesionales. Recordar utilizar siempre contraseñas robustas y el doble factor de autenticación siempre que sea posible.
- Mantener los sistemas operativos y las aplicaciones actualizados, tanto los que se usan profesionalmente como a nivel usuario. Instalar software de repositorios oficiales y no olvidar disponer de un antivirus actualizado.
- Cifrar los soportes de información para proteger los datos personales de la entidad de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.
- Realizar las copias de seguridad periódicas establecidas para garantizar la disponibilidad y resiliencia de los servicios y sistemas de información en caso de que ocurra cualquier incidente de seguridad o cualquier otro posible desastre (robo o pérdida del dispositivo, avería, etc.…). Comprobar regularmente que estas copias pueden restaurarse.
- En caso de necesitar acceder a la información almacenada en los equipos de la entidad, evitar el uso de aplicaciones de escritorio remoto. Estas herramientas pueden crear puertas traseras (backdoors) a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos. Además, al usar este tipo de aplicaciones aceptamos ciertos términos y condiciones de uso que podrían otorgar algún tipo de «privilegio» a las mismas sobre los equipos e información.
- En lugar de las aplicaciones de escritorio remoto, existen otras posibilidades de conexión a la entidad de forma segura a través de una red privada virtual o VPN, del inglés Virtual Private Network. De este modo, la información que se intercambia entre los equipos viaja cifrada a través de Internet.
- Asegurar que la configuración de la conexión wifi utilizada en el lugar de teletrabajo es correcta y segura. Así se evita que un ciberdelincuente pueda conectarse a ella y robar la información de la entidad o la de sus clientes.
- Recordar que en el teletrabajo también se debe garantizar, en todo momento, la seguridad de los datos personales y cumplir con las exigencias de seguridad marcadas por la normativa de protección de datos: Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPD-GDD).

- En caso de utilizar dispositivos móviles (smartphones, tablets, ordenadores portátiles, etc.) para acceder a la información corporativa, instalar aplicaciones de administración remota. En caso de robo o pérdida, permiten localizar el dispositivo o realizar un borrado de los datos si fuera necesario.
- Evitar el uso de redes wifi públicas (hoteles, cafeterías, aeropuertos, etc.), utilizar las conexiones 4G/5G en su lugar y acceder a servicios que utilicen comunicaciones seguras (SSL, HTTPS, etc.).
- Cuando la información deje de ser necesaria para la entidad, borrarla de forma segura. Si se trata de soportes no electrónicos (papel, negativos fotográficos, radiografías, etc.) será necesario utilizar una trituradora. Para los soportes electrónicos, utilizar el proceso de sobrescritura para reutilizar el dispositivo, o el de desmagnetización o destrucción física, en el caso de querer desecharlo.

Recomendaciones genéricas

- Tener instaladas las últimas actualizaciones del sistema operativo.
- Tener activados servicios de monitorización con alertas definidas.
- Revisar los registros y auditorías de las conexiones remotas.
- Tener habilitados canales de comunicación para reuniones mediante Internet.
- Restringir montar unidades mapeadas de la entidad en equipos remotos inseguros.
- Evitar las opciones de "Split-Tunneling" en equipos inseguros o que no cumplan todas las medidas de seguridad.
- Revisar o tener más vigilados unidades para intercambiar información.
- Asegurar si los antivirus escanean los dispositivos USB conectados a los equipos remotos si se bloquea el acceso de USB en dichos equipos.
- Tener listados telefónicos de fácil acceso para comunicarse con las diferentes personas.
- Tener listados de personas, direcciones IP, teléfonos, correos electrónicos corporativos y alternativos relacionados con el acceso a los sistemas de forma remota.
- Tener actualizado el listado de personas que pueden acceder remotamente a los equipos de la organización con la dirección IP de acceso y medio de conexión.

Control de acceso – seguridad física

Los trabajadores en régimen de teletrabajo, para garantizar unas medidas de seguridad equiparadas a la seguridad física implantadas en la propia entidad, deben:

- Evitar los accesos no autorizados al mobiliario, soportes o equipos con datos personales o información confidencial.
- Restringir la impresión, en el lugar de teletrabajo, de cualquier documentación interna de la entidad o de sus clientes.
- Restringir recoger documentación en formato papel de los propios clientes de la entidad. En caso de necesidad recoger dichos documentos, deberán ser enviados en el menor espacio de tiempo posible a las oficinas de la entidad a través de mensajero o, en caso de que esta posibilidad no sea viable, custodiar dichos documentos en un lugar cerrado y seguro.

Por lo tanto, la custodia y el acceso a la información, tanto de la propia entidad como de sus clientes, desde los lugares de teletrabajo debe restringirse a los sistemas de información de carácter informático (ordenadores portátiles, smartphones, etc.) a la que se tiene derecho como usuario de los sistemas de información de la entidad. Tanto los equipos (portátil, smartphone, etc.) como, en su caso, los soportes físicos (papel, etc.), deberán custodiarse en lugares y mobiliario de acceso restringido, de forma que personas no autorizadas puedan tener acceso a los mismos.

La información contenida en este documento ha sido obtenida, entre otras fuentes, del CCN-CERT e INCIBE:

- ***Cómo implantar una política de Acceso Remoto Seguro - https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/9638-como-implantar-una-politica-de-acceso-remoto-seguro.html***
- ***¿Tu casa también es tu oficina? ¡Protégela! - https://www.incibe.es/protege-tu-empresa/blog/tu-casa-tambien-tu-oficina-protegela***
- ****Teletrabajo: 5 consejos para reducir los riesgos de seguridad a empresas - https://bitness.pe/teletrabajo-consejos-reducir-riesgos-seguridad-empresas***
- ***Teletrabaje con seguridad - https://www.teletrabajo.gov.co/622/w3-article-4643.html***
- ***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***
- ***¿Por qué deberías utilizar una red privada virtual y cómo hacerlo? - https://www.incibe.es/protege-tu-empresa/blog/deberias-utilizar-red-privada-virtual-y-hacerlo***