GUÍA DE

BUENAS PRÁCTICAS DE CIBERSEGURIDAD

PARA EL TELETRABAJO

Bitdefender

ECUADOR

Guía de
Buenas Prácticas de Ciberseguridad para el Teletrabajo

Debido al estado de alarma provocado por el coronavirus, muchas empresas y organismos públicos están promoviendo el teletrabajo para garantizar la continuidad de sus funciones y servicios.

El teletrabajo, sin embargo, puede plantear riesgos de ciberseguridad, si no se había planificado con tiempo, no se ha formado adecuadamente al personal y no se han configurado de forma segura los equipos y las conexiones. Dado el contexto actual de urgencias, es posible que todo esto no se haya podido realizar en muchos casos; por este motivo ofrecemos una selección de las principales medidas de protección básicas a tener en cuenta que nos pueden ayudar a teletrabajar minimizando los riesgos de seguridad en el tratamiento de la información de nuestras organizaciones.

En necesario tener en cuenta que la situación actual es muy atractiva para los ciber delincuentes para robar contraseñas y secuestrar información confidencial a cambio de un rescate.

Esta selección se ha elaborado con el objetivo de facilitar una guía práctica y ejecutiva, dirigida a usuarios no expertos de administraciones públicas medianas y pequeñas, que no disponen de recursos para aplicar un plan completo y avanzado de seguridad. Queremos evitar un exceso de información y hacer recomendaciones no viables en las circunstancias en que nos encontramos. Para los usuarios que tengan interés en profundizar en este tema, facilitamos enlaces adicionales al final de la guía.

En esta guía, destacamos las medidas y soluciones de seguridad que permiten implantar ágilmente el acceso remoto a los recursos de una organización y ofrecer unas mínimas garantías de seguridad a la hora de teletrabajar:

1. Entornos y aspectos técnicos para teletrabajar de forma segura: Sistemas locales y basadas en la nube.
2. Pasos a seguir por los colaboradores o equipos para teletrabajar de forma segura.
3. Consejos para teletrabajar de forma segura.

1. Entornos y aspectos técnicos para teletrabajar de forma segura

La implementación de entonos de acceso remoto es todo un desafío desde la perspectiva de la seguridad y la gestión para cualquier organización. Las soluciones clásicas basadas en el despliegue de sistemas locales necesitan unas capacidades, tanto de personal como de infraestructura, que no siempre están disponibles en las organizaciones medianas o pequeñas.

No obstante, las organizaciones más grandes podrán adaptar sus sistemas actuales para implementar un sistema de acceso remoto seguro que pueda desplegar los servicios

necesarios y evitar vulnerabilidades por malware, botnets, ransomware, suplantación de identidad, atacantes, etc.

1.1. Solución Basada en los sistemas locales para teletrabajar seguro

La solución basada en los sistemas locales para teletrabajar de forma segura consiste en desplegar equipos portátiles configurados y gestionados por la organización en los que se use Internet como medio de acceso seguro a los servicios corporativos.

Esta solución requiere de múltiples mecanismos de seguridad que garanticen que todos los elementos TIC involucrados cumplan las medidas de seguridad establecidas para prevenir y evitar el riesgo de exposición de los sistemas a la hora de teletrabajar.

Las principales características de este sistema de teletrabajo son:

- Nivel de seguridad: Medio/Alto
- Infraestructura: Sistema local
- Sistema de autenticación: Certificados máquina/Simple
- Tiempo de puesta en producción: Alto
- Complejidad TIC: Alto
- Equipo de trabajo remoto: Portátil corporativo

Medidas de seguridad en el canal de comunicaciones

- La seguridad del canal de comunicaciones entre el propio equipo portátil corporativo y la red de la organización. Para establecer la comunicación es necesario confirmar la identidad del equipo, por ejemplo, a través de una comunicación VPN mediante autenticación con certificado de máquina (opción más habitual de conexión). Estas VPN deberán ser establecidas extremo a extremo entre el terminador de túneles del organismo y el endpoint.
- Para el establecimiento de dichas VPN se utilizarán protocolos seguros como IPSec o TLS 1.2 o superior. Proveerán autenticación de extremo a extremo, basada en la utilización de certificados digitales, protección de la integridad y, en el caso de que se maneje información sensible, protección de la confidencialidad. Las medidas de seguridad vinculadas a la validación de acceso deben ser revisadas con frecuencia para evitar duplicidades de acceso o se conozca la dimensión de estos.

Medidas de seguridad en los equipos clientes

1. Para teletrabajar, cada usuario utilizaría un equipo corporativo que incluyera, además de todas las medidas de seguridad estándar de la organización, medidas adicionales que permitan la comunicación con los servicios corporativos a través de Internet. Las medidas para registrar las actividades de los usuarios, así como sus conexiones son muy importantes para evitar posibles incidentes o facilitar su investigación posterior ya sea en materia pericial o de ciber inteligencia.

2. El cumplimiento de estas medidas de seguridad permitirá reducir la superficie de ataque y mitigar amenazas derivadas del teletrabajo:
    - **DMZ.** Todos los servicios a los que se tenga acceso en remoto deberán encontrarse en una DMZ. En esta DMZ se dispondrá de un proxy que controle el acceso a Internet.
    - **NAC.** Se deben utilizar las tecnologías de gestión de identidades a la hora de establecer distintos perfiles de permisos de acceso basados en las políticas de la organización. Como mínimo, se definirán dos tipos de perfiles: usuarios no privilegiados y administradores privilegiados.

Medidas de seguridad en el acceso a los servicios corporativos

1. Para el acceso a los servicios de la organización se plantean dos escenarios:
    - **Nivel Seguridad Alto -** Acceso a los servicios a través de Sistema VDI: cada usuario dispondrá de una máquina virtual que será un equipo de la propia organización.
    - **Nivel Seguridad Medio -** Acceso a los servicios a través de un Servidor de Escritorios Remoto (MTSC): los usuarios accederían a una especie de máquina virtual con acceso a los mismos servicios corporativos que tendrían en la oficina. Requiere del despliegue de un servidor con capacidad de dar servicio a todos los usuarios de la organización.

Medidas de seguridad en los endpoint

Por regla general, salvo causa justificada, deberán utilizarse:

- Herramientas EPP: en cualquier tipo de sistema.
- Herramientas EDR: recomendada para los sistemas que manejen información sensible.
- Herramientas ERM y ERA: Gestión de riesgos corporativos
- Herramienta de Sanbox Analizer

Estas herramientas deberán actualizarse con una periodicidad establecida por la política de seguridad de la organización y que dependerá del nivel de seguridad exigido por la información que vaya a manejar.

El endpoint deberá contar con las medidas de seguridad establecidas por la organización y, específicamente, deberán tenerse en cuenta las siguientes:

1. Medidas de Hardware:

- BIOS protegida con contraseña fuerte y configurada de acuerdo con el principio de mínima funcionalidad.
- Si son portátiles, dotados de filtros de privacidad (pantallas).

2. Medidas del sistema operativo:

- Autenticación fuerte y mediante directorio activo de la organización. En caso de que se vaya a manejar información sensible se recomienda doble factor de autenticación. Se bloqueará el equipo tras intentos fallidos de autenticación

consecutivos o después de un período de inactividad para evitar accesos no autorizados.
- Sistema operativo con soporte y parches de seguridad actualizados.
- Únicamente se podrá administrar el sistema desde un usuario administrador.
- Se implementará una configuración que restrinja y controle la ejecución de software de acuerdo con las políticas de la organización.

3. **Herramientas de seguridad:**

   Se instalarán herramientas antimalware. El software de detección de código dañino deberá configurarse para:

   - Analizar los ficheros procedentes de fuentes externas antes de trabajar con él.
   - Revisar el sistema cada vez que arranque y realizar escaneos regulares para detectar software malicioso.
   - Actualizar periódicamente las firmas de malware.
   - Implementar protección en tiempo real de acuerdo con las recomendaciones del fabricante.

4. **Cortafuegos personal.**

   Permite únicamente los flujos de comunicación autorizados conforme a las políticas de la organización y rechaza el resto. Evita que el equipo se conecte a otras redes no corporativas.

5. **ATC (Advanced Threat Control).**

   Es muy útil para sistemas que manejen información de nivel alto de seguridad. Su función es detectar y bloquear en tiempo real cualquier intento de intrusión en éste. El conjunto de reglas predefinidas y patrones de firma utilizados para detectar posibles ataques deberán ser personalizados y actualizados periódicamente conforme a la Política de Seguridad de la organización.

6. **Gestión de eventos.**

   Se utilizarán mecanismos para el registro de logs y eventos de seguridad generados por el sistema y/o los usuarios, que puedan ser almacenados y retenidos durante el período que establezca la Política de Seguridad establecida en la organización. La modificación de la referencia de tiempo será una función del administrador.

7. **Cifrado de datos.**

   Su función es proteger la confidencialidad e integridad de la información de los sistemas que almacenen información sensible. Concretamente, estos mecanismos serán:

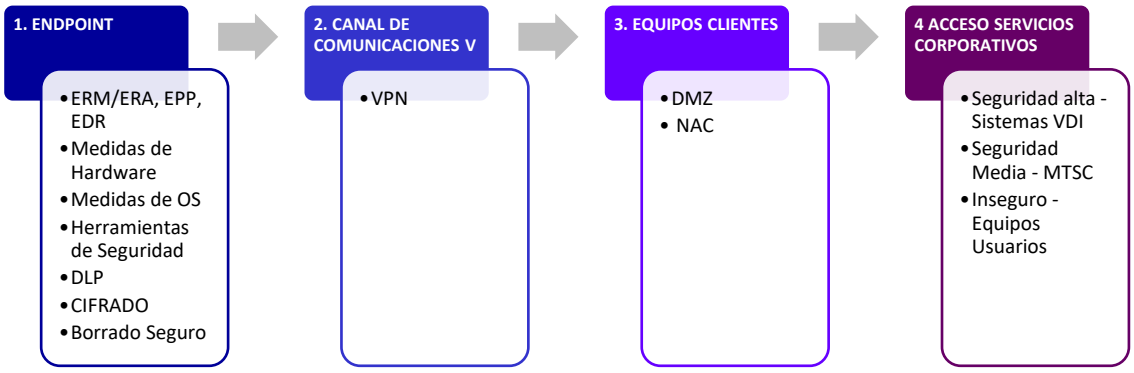
   - Cifrado off line: para la protección de la información sensible que vaya a ser enviada por o almacenada en un medio inseguro.
   - Cifrado at rest o cifrado de la información almacenada. Deberá utilizarse siempre que la solución de endpoint sea móvil o portátil para sistemas que guarden información sensible.

8. **Prevención de Fuga de Datos (DLP).**

   Siempre que sea posible, para sistemas que manejen información sensible, se aplicarán mecanismos que permitan controlar la salida de información desde el sistema.

9. **Borrado seguro.**

   Todos aquellos archivos que contengan información sensible deberán ser borrados de manera segura cuando finalice su uso utilizando un borrado seguro. El proceso consiste en una o varias pasadas de sobreescritura o el cifrado de la información. Medida que debe poder hacerse de forma telemática, especialmente para escenarios en los que un empleado demuestre ser infiel o deba ser despedido.



1.2. Solución basada en la nube para teletrabajar de forma segura

Las soluciones basadas en la nube para teletrabajar de forma segura consisten en desplegar una solución de acceso remoto seguro en la nube, a pesar de no disponer de una gran capacidad dentro de la organización que facilite temporalmente el acceso a la organización desde cualquier lugar con las medidas de seguridad necesarias.

Alguno de los beneficios de este tipo de sistemas son la autenticación de doble factor y poder dar seguimiento o tener la trazabilidad total de las conexiones realizadas por los usuarios remotos. Al aislarse completamente de la plataforma de acceso de red corporativa se impide que las vulnerabilidades presentes en el cliente pongan en riesgo a los sistemas e información corporativos a la hora de teletrabajar.

Las principales características de este sistema de teletrabajo son las siguientes:

- Nivel de seguridad: Medio/Alto
- Infraestructura: basada en soluciones Cloud
- Sistema de autenticación: Fuerte/Doble factor
- Tiempo de puesta en producción: Mínimo
- Complejidad TIC: Media/Baja
- Equipo de trabajo remoto: cualquiera con acceso a Internet

La arquitectura necesaria para proporcionar el teletrabajo (acceso remoto) recae principalmente en la infraestructura que se encuentra en la nube.

Medidas de seguridad del servicio en la nube

Las medidas de seguridad del servicio en la nube son las siguientes:

1. **Identity Management IM (suministrado por el Cloud):**

   Se deben utilizar las tecnologías de gestión de identidades a la hora de establecer distintos perfiles de permisos de acceso basados en las políticas de la organización. Como mínimo, se definirán dos tipos de perfiles: usuarios no privilegiados y administradores privilegiados. El control de accesos deberá permitir aplicar los siguientes criterios:

   - Todo acceso debe estar prohibido salvo concesión expresa.
   - Los privilegios de cada usuario o proceso se reducirán al mínimo para cumplir con sus obligaciones (principio de mínimo privilegio).
   - Cada usuario quedará identificado singularmente.
   - La utilización de los recursos deberá estar protegida.
   - La identidad del usuario deberá quedar previamente autenticada.
   - Exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por la organización.
   - Deberá implementar mecanismos de autenticación fuerte (doble factor) basada en certificados para acceder al servicio.

Notificación y respuesta ante incidentes.

Los proveedores conectados a la organización deben reportar todos los incidentes de seguridad detectados en sus instalaciones que afecten a los equipos prestadores de servicios, así como añadir información de las soluciones de eliminación y medidas de seguridad de los incidentes detectados.

Medidas de seguridad en el canal de comunicaciones

1. La parte del canal de comunicaciones entre la nube y los servicios corporativos se delegaría en los servicios Cloud

2. Se establecerán dos canales seguros:

   - Canal Organismo-proveedor de servicio en la nube. Deberán establecerse canales cifrados mediante la utilización de redes privadas virtuales (VPN). Estas VPN deberán ser establecidas entre el terminador de túneles del Organismo y el servicio en la nube. Para el establecimiento de dichas VPN se utilizarán protocolos seguros como IPSec o TLS 1.2 o superior.
   - Canal Proveedor de servicio en la nube-end point. El proveedor se encargará de dar acceso VPN mediante su tecnología y mecanismo de validación a sus usuarios. En este caso, serán canales https/TLS 1.2 o superior, al que serán de aplicación las indicaciones expuestas en el caso anterior.

Medidas de seguridad en los equipos

1. Cada usuario de la organización haría uso de su propio equipo TIC para acceder a través de una página web y una autenticación fuerte o doble factor de autenticación (por ejemplo, token software en el teléfono móvil, un SMS, etc.) a un portal en la nube que le daría acceso a los sistemas corporativos.

2. Los equipos de acceso a los servicios corporativos disponen de las mismas medidas de seguridad que las establecidas en la organización para el resto de sus equipos:

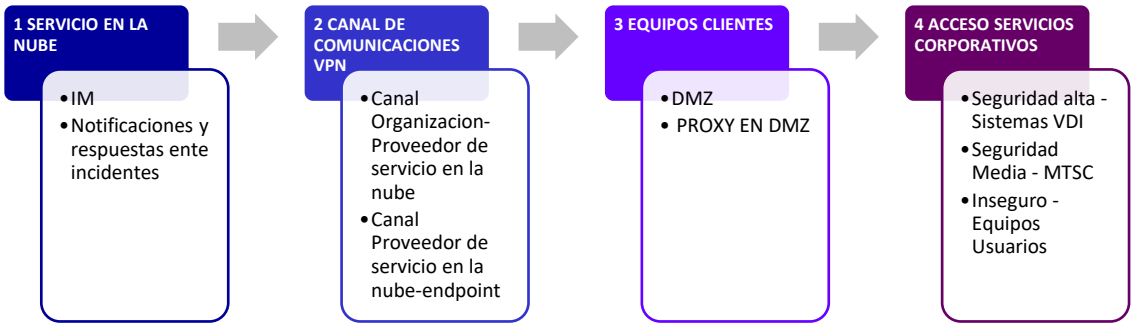
    - DMZ. Esta DMZ alojará al "Conector" y dará acceso a los servicios corporativos a los que se tenga acceso en remoto.
    - PROXY en DMZ. El acceso a Internet se gestionará a través de un servidor proxy a través de la red corporativa, aplicando las políticas de seguridad establecidas en la organización.
    - CONECTOR. Despliegue del conector Citrix dentro de la organización.

Medidas de seguridad en el acceso a los servicios corporativos

Para el acceso a los servicios de la organización se plantean tres escenarios:

1. **Nivel seguridad alto -** Acceso a los servicios a través de Sistema VDI: cada usuario dispondrá de una máquina virtual que será un equipo de la propia organización.
2. **Nivel seguridad medio** - Acceso a los servicios a través de un Servidor de Escritorios Remoto (MTSC): los usuarios accederían a una especie de máquina virtual con acceso a los mismos servicios corporativos que tendrían en la oficina.
3. **Inseguro** - Acceso directo a los propios equipos de los usuarios: este tipo de alternativas es desaconsejable al suponer un alto riesgo de infección por código dañino o ransomware. En caso de que sea la única alternativa posible, se deberían aplicar las siguientes medidas complementarias:

    - Restringir las direcciones IP desde donde se van a originar las conexiones.
    - Aumento de la gestión administrativa diaria para poder autorizar de nuevo cada una de las nuevas direcciones IP dinámicas que presentan los usuarios.
    - Contar con registros de auditoría asociados a las conexiones.



1.3. Pasos a seguir por los colaboradores o equipos para teletrabajar de forma segura

Es fundamental que los usuarios dispongan, diariamente, de sus portátiles o equipos para acceder remotamente a la organización en caso de activarse algún protocolo de actividad extraordinaria fuera de la oficina, dicho de otra manera, teletrabajo.

En estas situaciones que pueden ser provocadas por escenarios de crisis sanitarias como la del coronavirus, o por indisponibilidad de oficinas o desplazamientos profesionales, es conveniente llevar a cabo pruebas de conectividad para comprobar la funcionalidad del acceso remoto y registrar las direcciones IP, credenciales y accesos disponibles mediante la conexión remota.

Si para teletrabajar se debe dejar el equipo de la organización encendido, asegúrate de 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.
- Realizar análisis de los antivirus (exhaustivos) a los puestos de trabajo, aunque los ordenadores no se reinicien.
- Aplicar las actualizaciones programadas en la organización.
- Prever mecanismos que permitan el reinicio de los equipos de forma remota y acceder a través de canales establecidos desde fuera de la organización una vez reiniciado el equipo.

2. Consejos para teletrabajar de forma segura

A continuación, ofrecemos una lista de consejos de protección para teletrabajar de forma segura:

1. Evita navegar por páginas sin https, Deep Web o la Dark Web.
2. Evita realizar pagos online y, si lo haces, ten en cuenta los consejos de prevención del phishing y los consejos de seguridad bancaria online.
3. Evita o limita el acceso de equipos conectados entre sí o con la misma red, para evitar los riesgos de los wearables y el IoT.
4. Ten instaladas las últimas actualizaciones del sistema operativo.
5. Ten activados servicios de monitorización con alertas definidas.
6. Revisa los registros y auditorías de las conexiones remotas.
7. Ten habilitados canales de comunicación para reuniones mediante Internet.
8. Restringe montar unidades mapeadas del organismo en equipos remotos inseguros.
9. Evita las opciones de “Split-Tunneling” en equipos inseguros o que no cumplan todas las medidas de seguridad.
10. Revisa o ten más vigiladas unidades para intercambiar información.
11. Asegura si los antivirus escanean los dispositivos USB conectados a los equipos remotos o si se bloquea el acceso de USB en dichos equipos.

12. Ten listados telefónicos de fácil acceso para comunicarse con las diferentes personas.
13. Ten listados de personas, direcciones IP, teléfonos, correos electrónicos corporativos y alternativos relacionados con el acceso a los sistemas de forma remota.
14. Ten 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.

Estas recomendaciones son de carácter general. Si su organización dispone de una guía de ciberseguridad propia haga uso de ella.

3. Más información

A los usuarios que deseen ampliar esta información les recomendamos que visiten las siguientes páginas web especializadas:

- Bitdefender, Trabajo desde casa: Safety Tips https://hotforsecurity.bitdefender.com/blog/tag/covid-19
- Teleworking Quick Reference Guide, California Cyber Security Integration Center: https://www.caloes.ca.gov/LawEnforcementSite/Documents/Cal-CSIC_Advisory_Teleworking%20Guidance.pdf
- Guía de seguridad en el teletrabajo, Centre Seguretat TIC de la Comunitat Valenciana: https://concienciat.gva.es/wp-content/uploads/2018/03/infor_guia_de_seguridad_en_el_teletrabajo.pdf
- Cómo implantar una política de Acceso Remoto Seguro: Centro Criptológico Nacional (contenido avanzado): https://www.ccn.cni.es/index.php/es/actualidad-ccn/591-como-implantar-una-politica-de-acceso-remoto-seguro