Trabajo en Remoto

|Guía para un teletrabajo efectivo y seguro

pandasecurity.com/business/

/Contenido

1. Introducción 3

2. COVID-19: medidas de higiene y ciberseguridad 5

3. Consejos y buenas prácticas 9

4. Puntos clave de una política correcta: BYOD 11

5. Soluciones de monitorización hasta el endpoint 15

6. Contraseñas y cifrado 16

7. Conclusiones 17

panda

|Introducción

El trabajo en remoto se está convirtiendo rápidamente en uno de los principales beneficios que, a día de hoy, puede ofrecer una empresa a los empleados que integran su plantilla. En la última década, la tecnología ha evolucionado de tal forma que casi cualquiera puede realizar sus tareas diarias desde casa.

Las estadísticas sobre el teletrabajo muestran cómo **esta modalidad se ha expandido 10 veces más rápido** que otras áreas de la fuerza laboral. Las mismas estadísticas también nos dicen que los empleados a tiempo completo tienen cuatro veces más probabilidades de que se les ofrezca trabajo a distancia que a tiempo parcial. Los datos son rotundos: el número de personas que trabajan en remoto ha aumentado en un 140% desde 2005, lo que a nivel mundial se traduce en que el 52% de los trabajadores trabajan desde casa al menos una vez por semana. Es más, aquellos que trabajan a distancia al menos una vez al mes tienen un **24% más probabilidades de ser más felices y productivos** en el desempeño de sus funciones, mientras que el 21% de los trabajadores renunciaría a parte de su tiempo de vacaciones para obtener opciones de trabajo más flexibles.

Años

2005-2020

140%

Aumento de personas que trabajan en remoto

52%

De los trabajadores

Trabajan desde casa una vez por semana

panda

Paralelamente a las mejoras en las personas, también existen grandes ventajas para las empresas a la hora implantar el teletrabajo, como la disminución en un 25% de rotación de sus empleados en comparación con aquellas corporaciones que no permiten el teletrabajo, fomentando así la retención del talento. Permite optar a una mayor diversidad de perfiles y mejores candidatos a la hora de realizar procesos de selección, ya que permite conectar con más candidatos al poder realizar trabajos a distancia. Está probado que el trabajo remoto disminuye de forma directa el absentismo laboral, permitiendo al trabajador una disposición horaria mayor para gestionar su trabajo en beneficio de la conciliación laboral. Además, hay que tener en cuenta la importante reducción de costes, de hasta un 30%, por no necesitar infraestructuras de oficina.

30% Reducción de costes para las Empresas

A pesar de las múltiples ventajas que a primera vista puede aportar esta modalidad de trabajo al alza, **hay un alto porcentaje de empresas que aún se resisten a abrazar el teletrabajo por diversos motivos, como la seguridad.** En España sólo el 4,3% de los ocupados trabajaba habitualmente desde casa, según los datos de Eurostat de 2018, frente al 5,2 % de la media europea y por debajo de las tasas de países del entorno como Alemania (5%), Portugal (6,1%) y Francia (6,6%). En Estados Unidos, hay 4,3 millones de teletrabajadores, lo que representa sólo el 3,2% de toda la fuerza laboral del país. Todos están lejos de la experiencia de países como Holanda o Finlandia, donde el 14% y el 13,3%, respectivamente, de los ocupados teletrabaja. Según los datos que recoge la estadística del Ministerio de Trabajo, en España sólo 47 convenios colectivos (el 4 % del total) recoge entre sus cláusulas las condiciones para aplicar el teletrabajo a los 376.863 trabajadores que amparan (el 15,3 % de los que están bajo convenio).

Una cosa está clara: en la actualidad, los llamados millennials y la generación Z son sólo el 38% de la fuerza de trabajo, pero en 2028 serán el 58%. Teniendo en cuenta que son nativos digitales, y que no entienden un mundo sin una conectividad constante en todo momento y lugar, la utilización de dispositivos portátiles y móviles propios en la oficina y para el trabajo en general será cada vez mayor. **Esta tendencia tiene consecuencias más allá del mercado del consumo y afecta al entorno corporativo conforme las nuevas generaciones se van incorporando al mercado de trabajo.** En este sentido, la consultora Markets & Markets calcula que el mercado de Bring Your Own Device (BYOD) alcanzará 73.300 millones de dólares en 2021, siendo ya un porcentaje considerable de la plantilla trabajadores en remoto.

BYOD **73.300** millones $ en **2021**

panda

Y ahora, adelantándonos **a las estadísticas y de improviso, llega el virus COVID-19 y es capaz de provocar por sí mismo que quienes llevan años resistiéndose a todo tipo de cambios en la adopción del trabajo en remoto en el seno de las organizaciones, ahora se manifiesten a favor** del teletrabajo; por responsabilidad o por imposición. Sea cual sea el motivo, en estos días aumenta considerablemente el número de dispositivos conectados fuera del perímetro de la oficina, y surgen las dificultades propias derivadas de esta situación a las que se enfrentarán aquellas compañías que no tengan experiencia previa ni la tecnología adecuada.

|COVID-19: medidas de higiene y ciberseguridad

La complejidad técnica y un perímetro cada vez más disperso han ampliado la superficie de ataque en los últimos años. Por ello, **aunque la seguridad perimetral sigue siendo la primera barrera para frenar ataques, la seguridad del endpoint se ha convertido en un asunto de vital importancia para proteger a la empresa**, ya que es donde se almacena prácticamente la totalidad de archivos e información sensible. Ahora hay que asegurar la protección de un sinfín de endpoints, como portátiles, móviles, tablets y multitud de dispositivos del Internet of Things (IoT). Y más en los tiempos que corren.

La seguridad del endpoint se ha convertido en un asunto de vital importancia para proteger a la empresa >

Y mientras el mundo entero trabaja para prevenir la propagación del coronavirus, las organizaciones están trasladando a sus empleados a un modelo de trabajo en remoto a velocidades nunca vistas. Derivado de estas prácticas de teletrabajo y de **las conexiones que se abren para facilitar la comunicación entre empresa y empleados, los sistemas de las organizaciones en general, están poniendo a prueba la capacidad técnica de nuestro tejido empresarial**. Sumado a la tensión que esto supone para los equipos de IT, las arquitecturas de red y los proveedores, ahora se plantean nuevos retos en ciberseguridad.

Al mismo tiempo, **los ciberdelincuentes están ocupados usando nuevas tácticas y técnicas diseñadas para explotar esta situación global de confusión y caos,** planteando problemas críticos de seguridad informática. La sociedad está tan pendiente de tener información actualizada sobre esta enfermedad, que abren de forma compulsiva en su ordenador o en su móvil cualquier mensaje, email, audio o archivo que reciben sobre el coronavirus. Y esto es bien sabido por los *black hat.*

El enorme aluvión de mensajes en internet se ha convertido en el camuflaje perfecto para que los ciberciminales nos cuelen algún virus informático sin que nos demos ni cuenta. Desde que se comenzó a hablar de la enfermedad se han registrado alrededor de 4.000 nuevos dominios en Internet relacionados con el término coronavirus, de los cuales al menos la mitad son potencialmente peligrosas en términos de ciberseguridad. Si a todo ello le sumamos las otras tantas miles de cuentas de redes sociales que se han dado de alta y los millones de mensajes que circulan en la red, podemos afirmar que **toda actividad digital relacionada con el CoVID-19 supone el caldo de cultivo perfecto para que los ciberdelincuentes extiendan una red potencial de ciberamenazas.**

Algunos intentan hacerse pasar por instituciones públicas que mandan información acerca del virus; otros ciberataques están diseñados para parecer una orden de compra de mascarillas, para así hacer repercutir en un envío directo de dinero a los cibercriminales. También se han visto casos que prometen información acerca de la política de empresa en cuanto al teletrabajo para intentar robar credenciales.

Sin ir más lejos, se ha localizado una campaña en la que se están enviando mensajes con el asunto “Atención coronavirus” que instala un malware a través de Microsoft Office para abrir una ‘puerta trasera’ al ordenador desde el que pueden asaltar a la víctima. Asimismo, desde este lunes, se pueden observar nuevos envíos masivos de emails que dirigen a una web de phishing en la que un virus informático llamado Remcos RAT está infectando los dispositivos de los usuarios. El ataque se lleva a cabo por medio de un supuesto archivo PDF denominado “Medidas de seguridad ante el Coronavirus”. Sin embargo, al abrir el archivo se ejecuta el malware.

También se ha detectado un grupo APT que **lleva a cabo una campaña de spear phishing**, utilizando la pandemia para propagar el malware del grupo. Los emails dicen contener información acerca del coronavirus, pero en realidad contienen dos archivos RTF (Rich Text Format) maliciosos. Si la víctima abre estos archivos, se lanza un RAT (Remote access trojan) que es capaz de hacer capturas de pantalla, elaborar listas de archivos y directorios en el equipo y descargar archivos entre otras capacidades. Para convertir este archivo en una ciberarma, los atacantes utilizaron RoyalRoad, una herramienta popular entre los actores de amenaza chinos, que les permite a crear documentos personalizados con objetos incrustados, que pueden explotar vulnerabilidades en Equation Editor, la herramienta que se utiliza para crear ecuaciones complejas en Word. La arquitectura de este malware, que tiene parecidos con un plugin, sugiere que existen otros módulos, además del payload que se ha visto en esta campaña.

Amenazas tradicionales, como el ransomware, siguen especialmente activas. Se han visto diversas campañas que aprovechan la pandemia para infectar a sus víctimas, y el notorio botnet Emotet y el troyano TrickBot también **han explotado la situación** para llegar a incluso más sistemas.

/CEO

Hay muchas posibilidades de que un cibercriminal esté suplantando su identidad y nos mande hacia una página de phishing]

Y es que además de los ciberincidentes que explotan esta situación, hay ciertos incidentes que tienen un impacto directo sobre los afectados por la pandemia, afectando infraestructuras tan críticas como los centros de investigación donde se está trabajando a contrarreloj. Hacen unos días, en la Republica Checa, el centro de investigación del Hospital Universitario de Brno **se vio obligado a detener sus actividades debido a un ciberataque.**

Por si fuera poco, gran parte de las empresas está enviando emails de forma masiva a todos sus clientes, colaboradores y proveedores para informarles de que, pese al coronavirus, siguen operativas. En este sentido, aunque debemos leer esos emails en los que el CEO de una compañía asegura que está afrontando con fortaleza el CoVID-19, hay que **desconfiar de todo mensaje que incluya enlaces externos**. Porque lo más probable es que el directivo de esa compañía sea quien dice ser.

Pero, **hay muchas posibilidades de que un cibercriminal esté suplantando su identidad y nos mande hacia una página de phishing** o que ese enlace instale en nuestro equipo un malware con el que nos puedan secuestrar toda nuestra información.

Estos ataques están cada vez más preparados para vulnerar la seguridad de nuestros endpoints. Por todo ello, hay que extremar la precaución ante cualquier email o mensaje en el que nos deriven a una página web en la que tengamos que tomar alguna medida como consecuencia directa o indirecta del coronavirus.

En este contexto de inestabilidad, **¿cómo se puede mantener una ciberseguridad eficiente y eficaz entre todos los trabajadores trabajando en remoto?**

panda

|Consejos y buenas práticas

Queda claro que si los empleados manipulan datos desde sus casas, las compañías no tienen tanto control sobre las medidas de protección, y por ello temen que se produzcan pérdidas de información. El temor es lógico. Un entorno doméstico puede llegar a ser mucho más peligroso que el corporativo, en el que el propio software de los servidores ofrece garantías de seguridad.

Los riesgos existentes son muchos y muy variados. La pérdida de datos puede producirse de diferentes formas: un fallo en el equipo que borre archivos de los que no hay una copia de seguridad, así como el robo de una contraseña o incluso el del equipo en sí, que puede hacer que el ladrón termine con información empresarial confidencial en su poder.

No obstante, el teletrabajo no tiene que ser sinónimo de peligro. Eso sí, para que las empresas permitan que sus empleados se lleven trabajo a casa con total tranquilidad, primero es imprescindible que exista un protocolo que establezca cómo actuar al trabajar en remoto en lo que a seguridad se refiere, teniendo en cuenta que ahora el perímetro a securizar llega hasta ahí donde esté un trabajador. Por eso, la firma de análisis Cybersecurity Ventures estima que el gasto global en ciberseguridad alcanzará el billón de dólares en los próximos cinco años.

Sin embargo, muchas de estas inversiones en ciberseguridad sólo protegen los dispositivos y servidores de la red corporativa y **con el BYOD queda patente que la protección del perímetro físico ya no es suficiente.** Hay que tener en cuenta que la organización que realiza el despliegue debe realizar un análisis del nivel de seguridad requerido para la información que se va a manejar en los puestos de trabajo remotos o móviles. La implementación de una solución de acceso remoto es un reto desde el punto de vista de la seguridad y la gestión para cualquier organización. Las soluciones clásicas basadas en el despliegue de sistemas locales u on-premise requieren de capacidades, tanto de personal como de infraestructura, que no siempre están disponibles en organizaciones medianas o pequeñas.

/Escenarios de trabajo en remoto:

BYOD

Bring Your Own Device.

En un escenario BYOD, el usuario final es propietario del dispositivo (teléfono móvil, Tablet, portátil), donde el Administrador IT de la organización genera un Workspace, también llamado contenedor o Perfil de Trabajo (WorkProfile), dentro del cual exclusivamente administra políticas y restricciones de seguridad, a través de una aplicación agente dentro del Workspace, mediante una aplicación especial agente (Profile Owner).

COPE

Corporate Owned Personal Enabled.

En los escenarios COBO y COPE el dispositivo (teléfono móvil, Tablet, portátil) es propiedad de la organización, y el Administrador IT tiene acceso a control total del dispositivo, implementando políticas de seguridad y restricciones. En el escenario COPE, existe una aplicación agente en el área personal, denominada DO (Device Owner), que realizará la configuración de políticas en el conjunto del dispositivo, como por ejemplo WiFi, además de restricciones en el área personal del usuario, normalmente restricciones mínimas y básicas de seguridad. Al ser un escenario COPE, existirá también un Workspace, con su agente gestor denominado (Profile Owner) dentro de él. El Administrador IT de la organización, realizará una configuración de seguridad más estricta en Workspace/Contenedor, que complementará la configuración básica del área personal del usuario.

COBO

Corporate Owned Business Only.

El escenario COBO, se utiliza en despliegues que requieren mayor seguridad, donde el usuario final no dispone de área personal, ya que el conjunto del dispositivo está fuertemente restringido. En un escenario COBO, solamente existe un agente DO, y ningún Workspace/Contenedor es creado.

panda

Es fundamental, por tanto, que la estrategia de BYOD incluya directrices específicas y criterios claros.

Una vez establecidos estos criterios de uso de los programas, el responsable de TI debe aprobar qué empleados pueden añadirlos a sus dispositivos personales. Por otro lado, no se trata de que el departamento de TI tenga un control férreo del contenido de los dispositivos de los empleados.

La situación ideal es llegar a un **equilibrio entre mantener la seguridad de los datos de la empresa y salvaguardar la privacidad de los empleados**, que continuarán usando sus dispositivos para cuestiones personales.

Por ello, las políticas excesivamente restrictivas o invasivas son contraproducentes.

Con el BYOD queda patente que la protección del perímetro es insuficiente}

Buscar el equilibrio entre la seguridad de los de la empresa y la privacidad de los empleados >

|Puntos clave de una política correcta: BYOD

/Recomendaciones OMS:

Lávese las manos con frecuencia Limpie sus manos de forma regular y a fondo con un frotador de manos a base de alcohol o lávelas con agua y jabón.

¿Por qué? Lavarse las manos con agua y jabón o con un desinfectante para manos a base de alcohol mata los virus que puedan estar en sus manos.

Mantener el distanciamiento social: Mantenga al menos 1 metro (3 pies) de distancia entre usted y cualquier persona que esté tosiendo o estornudando.

¿Por qué? Cuando alguien tose o estornuda, se rocían pequeñas gotas de líquido por la nariz o la boca que pueden contener el virus. Si está demasiado cerca, puede respirar las gotitas, incluyendo el virus COVID-19 si la persona que tose tiene la enfermedad.

Evite tocarse los ojos, la nariz y la boca

¿Por qué? Las manos tocan muchas superficies y pueden recoger virus. Una vez contaminadas, las manos pueden transferir el virus a los ojos, la nariz o la boca. Desde allí, el virus puede entrar en tu cuerpo y puede enfermarte.

panda

/Medidas prácticas para mitigar riesgos cibernéticos:

Conectarse a través de una VPN a la red interna de la empresa, evitando el uso de redes wifi públicas o de terceros

La concienciación y formación previa y continua de los empleados, como no podía ser de otra manera, se convierte en un elemento fundamental en este tipo de crisis.

Al igual que cuando uno está en la oficina, acceder únicamente a sitios web que utilizan HTTPS, ofreciéndonos una conexión segura; así como preocuparnos por que todas las contraseñas que protegen el acceso a las cuentas sean robustas e individuales.

Practica la higiene respiratoria: Asegúrate de que tú, y la gente que te rodea, sigan una buena higiene respiratoria. Esto significa cubrirse la boca y la nariz con el codo doblado o con un pañuelo de papel al toser o estornudar. Luego deseche el pañuelo usado inmediatamente.

¿Por qué? Las gotas propagan el virus. Al seguir una buena higiene respiratoria, se protege a las personas que le rodean de virus como el del resfriado, la gripe y el COVID-19.

Si tiene fiebre, tos y dificultad para respirar, busque atención médica de inmediato.Quédate en casa si te sientes mal. Si tiene fiebre, tos y dificultad para respirar, busque atención médica y llame con antelación. Siga las instrucciones de su autoridad sanitaria local.

¿Por qué? Las autoridades nacionales y locales dispondrán de la información más actualizada sobre la situación en su zona. Llamar con antelación permitirá a su proveedor de atención médica dirigirle rápidamente al centro de salud adecuado. Esto también le protegerá y ayudará a prevenir la propagación de virus y otras infecciones.

Manténgase informado sobre los últimos desarrollos de COVID-19. Siga los consejos de su proveedor de atención médica, su autoridad de salud pública nacional y local o su empleador sobre cómo protegerse a sí mismo y a los demás de COVID-19.

¿Por qué? Las autoridades nacionales y locales tendrán la información más actualizada sobre si COVID-19 se está propagando en su zona. Son los más indicados para asesorar sobre lo que la gente de su zona debería hacer para protegerse.

Las soluciones de ciberseguridad deben ser avanzadas y estar actualizadas, considerando utilizar programas de detección y respuesta en los endpoint para limitar a distancia el impacto de un dispositivo en peligro. Las soluciones de seguridad avanzada deben incluir capacidades de EPP y/o capacidades EDR completas que monitorizan la actividad en el endpoint y ofrecen una visibilidad continua, integral y detallada. Esta monitorización es la base del servicio Zero-trust App Service, único en el mercado.

Las empresas deberían examinar, evaluar y actualizar, de ser necesario, sus planes de respuesta a incidentes y de continuidad de las actividades. Nuestros servicios de respuesta a incidentes comienzan a menudo mediante la implementación de nuestros agentes en los endpoints del cliente lo cual proporciona visibilidad de indicios de presencia de atacantes en su red y sobre los activos se han sido comprometidos. En base a ellos se establece plan de remediación personalizado, proporcionando una estrategia para erradicar los atacantes fuera de la red.

Realiza copias de seguridad de forma periódica para asegurar que la información no se pierda en caso de incidente”. Incluso en el peor de los escenarios, siempre tendrás la posibilidad de recuperar los datos, que son el sustento de las empresas.

/ Otras recomendaciones >

- Tener habilitados **canales de comunicación** para reuniones mediante **Internet**.
- **Cerrar** todas las conexiones que no sean **estrictamente necesarias**.
- Evitar las opciones de **“Split-Tunneling”** en equipos inseguros o que no cumplan todas las medidas de seguridad.
- Prever mecanismos que permitan el reinicio de las máquinas de forma remota y acceder por canales establecidos a las mismas desde fuera de la organización una vez se reinicie el equipo.
- Realizar **análisis programado de los antivirus** (exhaustivos) en los puestos de trabajo, aunque los ordenadores no se reinicien.
- Restringir montar **unidades mapeadas del organismo** en equipos remotos inseguros.
- Cerrar todas las aplicaciones cuando **no se estén utilizando**.
- Aplicar las **actualizaciones programadas en la organización**, para ello puede ser necesario apagar y encender los equipos de forma periódica.
- Tener **listados** de personas, direcciones IP, teléfonos, correos electrónicos corporativos y alternativos relacionados con el **acceso a los sistemas de forma remota**.
- Tener **listados telefónicos** de fácil acceso para comunicarse con las personas de diferentes áreas.
- Tener activados servicios de monitorización con alertas definidas.
- Revisar o tener más vigilados **unidades para intercambiar información**.
- 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.
- Asegurar si las soluciones de ciberseguridad escanean los **dispositivos USB** conectados a los equipos remotos o si se bloquea el acceso de USB en dichos equipos.
- Revisar los **registros y auditorías** de las conexiones remotas.

panda

* Puntos compartidos con aquellas medidas publicadas por el CCN-CERT en su «Abstract» que lleva por título: «Medidas de seguridad para Acceso Remoto».

|Soluciones de monitorización hasta el endpoint

Dada la naturaleza de los riesgos de seguridad que puede entrañar el trabajo en remoto, las organizaciones deberían implementar soluciones que apliquen una monitorización constante y en tiempo real de la red corporativa y de todos sus elementos de acceso.

Porque hoy en día, los equipos de ciberseguridad están asumiendo demasiadas tareas, en especial los responsables de seguridad informática. Y esta carga tan alta de trabajo hace que las verdaderas amenazas, puedan quedarse en un segundo plano y dejen de ser atendidas de manera efectiva, poniendo en riesgo la seguridad de la propia compañía.

El trabajo en remoto asumido en estos días hace que la seguridad debe ser abordada con un servicio de detección y respuesta en el endpoint capaz de clasificar cada una de las aplicaciones de las organizaciones de forma precisa y de bloquear amenazas avanzadas, ataques dirigidos y zero-day que otras soluciones tradicionales no son capaces de detectar.

No olvidemos que, aunque el BYOD presenta nuevos riesgos de seguridad, son mucho mayores las oportunidades que ofrece para las empresas y empleados si lo adoptan con las necesarias medidas de precaución.

Una prevención de riesgos basada en políticas adecuadas y en soluciones de monitorización en tiempo real que alcancen a todos los dispositivos es la mejor manera de aprovechar todo el potencial del trabajo en remoto.

panda

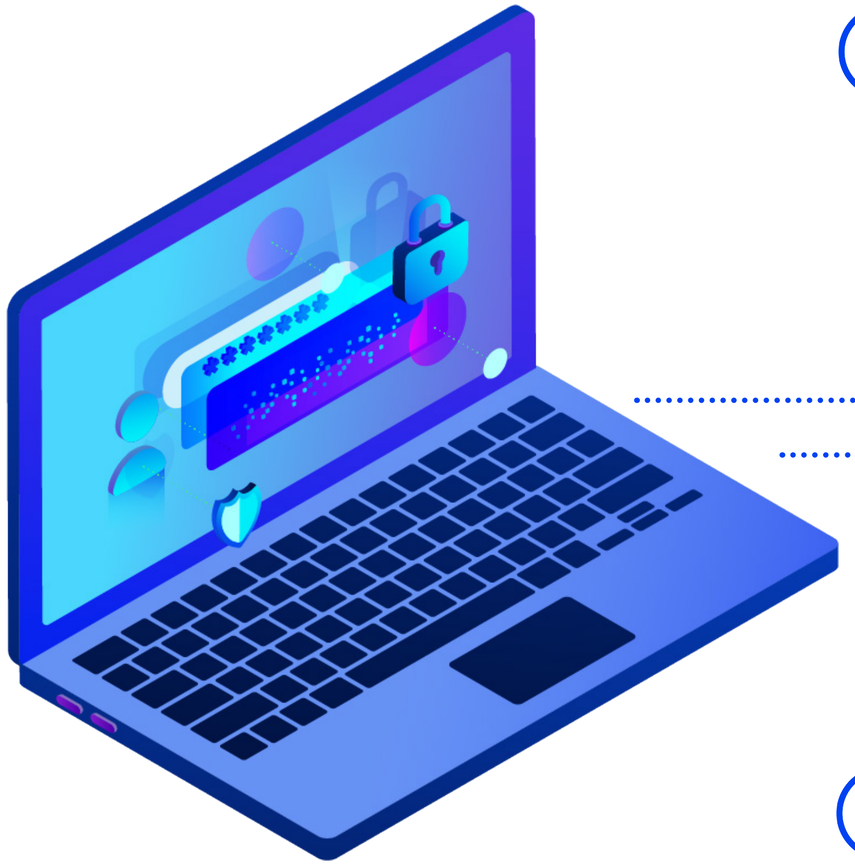
|Contraseñas y cifrado

Otro punto clave para que el teletrabajo sea seguro son las **contraseñas**. El robo de la que utilizan los empleados para acceder a la red de la empresa de forma remota puede resultar un incidente de seguridad crítico, ya que pondría en bandeja a los ciberdelincuentes una gran cantidad de información.

Más allá de la contraseña del servidor corporativo, los trabajadores que desempeñen su función desde casa deben tener en cuenta que, a la hora de utilizar servicios y herramientas en la nube, es importante seguir ciertos consejos para construir contraseñas seguras y fiables: **no repetir contraseña, cambiarla cada cierto tiempo y utilizar un gestor de contraseñas es fundamental para evitar que nos las roben.**

No obstante, las contraseñas no siempre son suficientes. Si bien un escritorio remoto es útil para evitar almacenar **información corporativa** en el ordenador de tu casa, en ocasiones es inevitable guardar algo en el equipo.

En este caso, además del uso de contraseñas seguras, es **importante cifrar la información confidencial.** Así, se evita que la pérdida (o el robo) del portátil suponga también el robo de datos. Cifrando archivos concretos a través del sistema operativo o cifrando el disco duro al completo, se acaba el riesgo.



- No repetir contraseñas
- Cambiar la contraseña cada cierto tiempo

panda

|Conclusiones

¿Qué debes pedirle a una solución de ciberseguridad para proteger tu dispositivo en el trabajo en remoto?

1-Bloquear amenazas conocidas y desconocidas de forma preventiva

Para evitar las brechas de seguridad, debe producirse un cambio: pasar de detectar y responder a incidencias después de que ocurran a evitar que se produzcan estas brechas en primer lugar. Los endpoints deben estar protegidos frente a amenazas conocidas, desconocidas y de día cero enviadas mediante malware y exploits a equipos que pueden estar con o sin conexión, en las instalaciones o fuera de ellas y conectados a la red de la organización o no. Un paso clave para lograrlo consiste en incorporar análisis de amenazas local y basado en la nube para detectar y evitar amenazas desconocidas.

2-No afectar negativamente a la productividad de los usuarios

Una solución de seguridad avanzada del endpoint debe permitir que los usuarios finales lleven a cabo su labor diaria y usen las tecnologías móviles y basadas en la nube sin temor a infectarse. Deberían poder centrarse en sus responsabilidades en lugar de tener que preocuparse por parches de seguridad y actualizaciones. Por último, deberían tener la seguridad de que están protegidos frente a malware o exploits que se ejecuten sin saberlo y que puedan poner en riesgo la seguridad de sus sistemas.

Debe permitir que los usuarios lleven a cabo su labor diaria y usen las tecnologías móviles y basadas en la nube sin temor a infectarse[

panda

3-Convertir automáticamente la inteligencia sobre amenazas en prevención

La inteligencia sobre amenazas obtenida gracias a afrontar ataques nuevos deben permitir que los agentes del endpoint impidan de forma instantánea el malware conocido, identifiquen y bloqueen el malware desconocido e impidan que ambos infecten los endpoints. Asimismo, los datos sobre amenazas deben recopilarse dentro de la organización: red, nube y endpoint. La automatización debe utilizarse para establecer una correlación entre los datos, reconocer indicadores de peligro, crear protecciones y expandirlas en toda la organización.

4-Proteger todas las aplicaciones

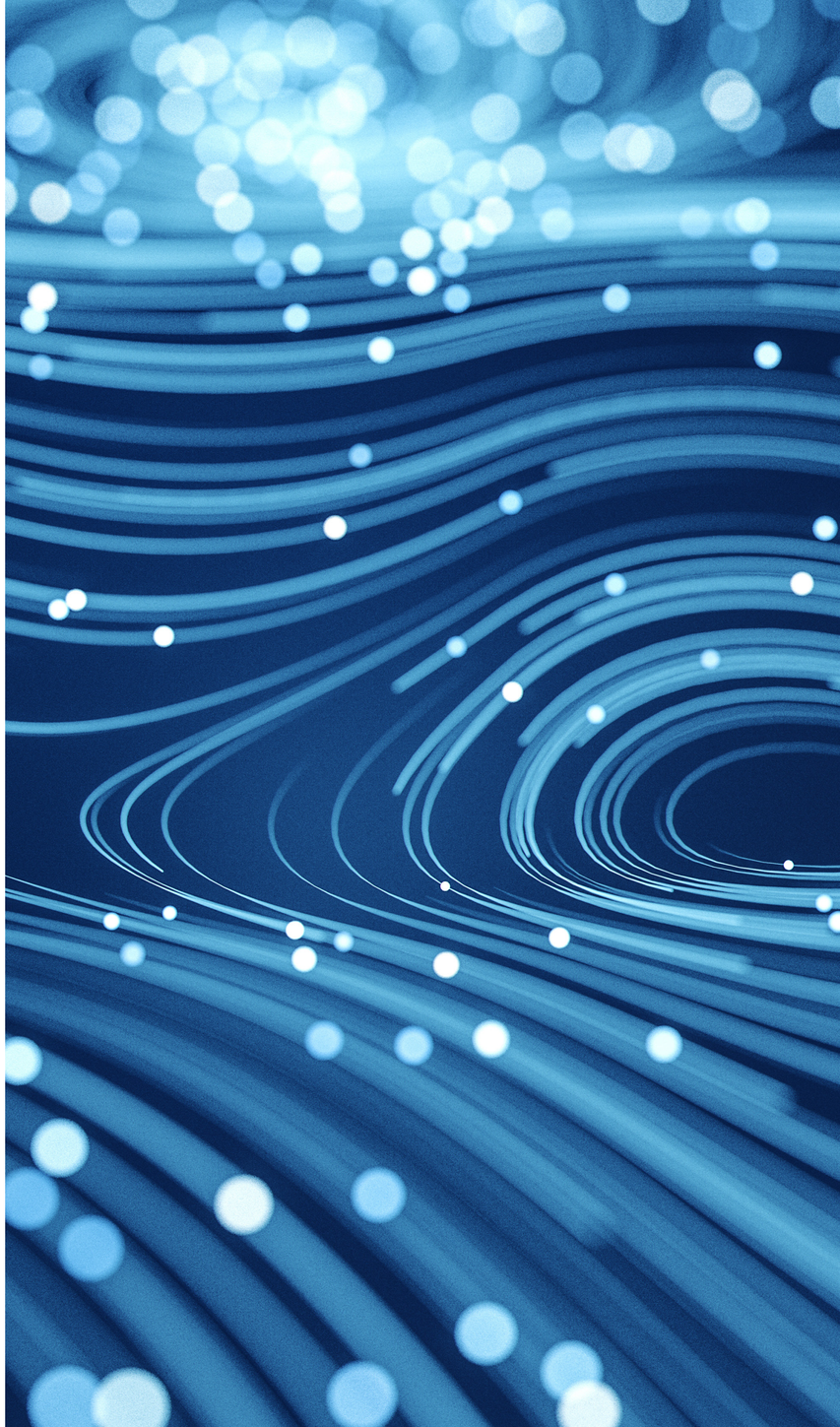
Los errores o fallos en las aplicaciones proporcionan a los cibercriminales una gran área de ataque que los antivirus tradicionales no pueden proteger. La infraestructura de seguridad de una organización debería poder ofrecer protección total contra exploits a todas las aplicaciones, incluidas aplicaciones de terceros y propias. También debería poder agilizar el proceso de aprobación de aplicaciones nuevas a medida que se instalan en el entorno mediante la emisión de respuestas rápidas de seguridad.

5-Evitar que la seguridad afecte al rendimiento del sistema

Las soluciones de seguridad no deberían suponer una carga para los recursos del sistema, como la RAM, la CPU o el espacio de almacenamiento en disco. La protección del endpoint debe ser lo suficientemente ligera para no necesitar muchos recursos del sistema o entorpecerá el rendimiento del sistema y degradará la experiencia del usuario.

6-Proteger los sistemas anteriores

Es posible que las organizaciones no siempre instalen las actualizaciones del sistema y los parches de seguridad en cuanto están disponibles. Ello puede deberse a que, al hacerlo, interferirían, disminuirían o eliminarían capacidades operativas fundamentales, o bien a que los parches no estén disponibles para sistemas y programas anteriores que hayan llegado al final de su vida útil. Una solución de seguridad del endpoint completa debe dar soporte también a sistemas donde no se puedan instalar parches evitando la explotación de vulnerabilidades, conocidas o desconocidas, de los programas, con independencia de la disponibilidad o aplicación de los parches de seguridad.



7-Estar preparada para su uso en el ámbito empresarial

La seguridad del endpoint debería dar soporte a la forma en que una empresa implementa sus recursos informáticos e integrarse en ella, ampliarse a tantos endpoints como sea necesario y admitir implementaciones que abarquen entornos dispersos geográficamente. Asimismo, debe ser flexible en lo que respecta a brindar una protección amplia mientras sigue dando soporte a las necesidades empresariales sin restringir en exceso la actividad. Esta flexibilidad es fundamental, ya que las necesidades de una parte de la organización pueden ser totalmente distintas a las de otra. Además, la solución debe poder ser gestionada fácilmente por el mismo grupo que gestiona la seguridad en otras partes de la organización. Debe estar diseñada teniendo presente la gestión empresarial, sin añadir carga operativa.

8-Proporcionar verificación independiente de los requisitos de cumplimiento normativo del sector

Con frecuencia, el cumplimiento normativo exige que las organizaciones que se encuentren dentro de una jurisdicción determinada implementen programas antivirus para proteger sus endpoints. Para proteger de forma proactiva los endpoints sin dejar de satisfacer los requisitos de cumplimiento normativo, como las últimas normativas generales de protección de datos (GDPR), los proveedores de seguridad del endpoint que sustituyan las soluciones antivirus existentes deberían poder facilitar la validación de terceros para ayudar a los clientes a conseguir o mantener el cumplimiento.

9-Proporcionar verificación independiente como sustitución del antivirus

Cualquier producto de seguridad destinado a sustituir al antivirus existente debería verificarlo y validarlo idealmente un tercero independiente en lo que respecta a su rendimiento. Las revisiones independientes aportan un elemento de control esencial con el que no pueden contar las organizaciones que pretenden sustituir el antivirus.

10- Estar reconocido por el mercado y analistas del sector.

Cualquier empresa que desee implementar una solución de ciberseguridad avanzada debería asegurarse de que la solución de esté avalada en el ámbito de la seguridad del endpoint por un analista o una empresa de investigación acreditados. De este modo, se tiene la seguridad de que la solución y su proveedor cumplen los requisitos estándar en cuanto a viabilidad como proveedor de seguridad del endpoint.

panda

Contacta con nosotros]

pandasecurity.com/business/

More info at: www.pandasecurity.com/business/