TELETRABAJO

Seguridad Cloud para la continuidad del negocio

2020

TELETRABAJO

Seguridad Cloud para la continuidad del negocio

El teletrabajo supone tener que acceder a datos, información e incluso aplicaciones y software alojados en la nube, lo que pone en riesgo uno de los activos más críticos de cualquier organización. La infraestructura en la nube permite seguir con las funciones y labores del día a día, pero también supone una oportunidad para los cibercriminales, que buscarán en esta modalidad de trabajo el acceso a los recursos y activos de la organización, hecho que cualquier organización ha de afrontar con el objetivo de mantener a buen recaudo el valioso activo de la información.

Desde **Grupo Oesía** trabajamos para que el teletrabajo se realice de forma segura y, por ello, ofrecemos una solución de seguridad complementaria para proteger los entornos basados en la nube y que todos los miembros de la organización puedan continuar con sus labores diarias.

Para ello, nos apoyamos en tecnología de nuestro partner **Check Point Software Technologies**, considerada una de las empresas líderes en el mercado.

Retos a los que nos enfrentamos al teletrabajar en entornos CLOUD:

Al igual que exigimos cumplir la normativa y políticas de seguridad cuando trabajamos en las oficinas de la organización, debemos asegurar que el conjunto de profesionales de la compañía continúe aplicando estas medidas en remoto, a

pesar de no disponer de los mismos recursos. El acceso a internet y a las herramientas corporativas es algo que está prácticamente asegurado en nuestros hogares, pero al igual que en las oficinas de la organización, tenemos que aplicar una serie de medidas para realizarlo de forma segura.

Estamos ante una situación que nos exige la revisión de la normativa y políticas de seguridad en relación al acceso remoto de dichas herramientas corporativas y la información que manejamos. Surge la necesidad de actualizar nuestras medidas y anticiparnos a la actividad de los cibercriminales. Algunos de los retos que enfrenta el teletrabajo son los siguientes:

- **Suplantación de identidad (Phishing):** Hemos de tener cuidado con la comunicación electrónica que recibimos y verificar el remitente, enlaces incluidos en el mensaje, contenido adjunto que podamos encontrar y el propio contenido del mensaje. Tenemos que ser críticos y dudar de los dominios sospechosos, puesto que los ciberdelincuentes usan la ingeniería social lograr sus objetivos.
- **Protección de datos:** Debemos asegurarnos de que la información que manejamos con las herramientas corporativas está protegida en todo momento y no supone un riesgo para nuestra organización, de lo contrario, estaremos exponiendo el duro trabajo realizado a delincuentes que aprovechan estas situaciones de confusión para perpetrar sus objetivos.
- **Desconfiemos:** No supongamos nada, verifiquemos. Hemos de comprobar la información, quién tiene acceso a la misma, quién puede dar dichos accesos y asegurarla mediante la autenticación multifactor.
- **Gestión de riesgos:** Los administradores han de tener informes sobre los riesgos de los entornos Cloud para poder tomar acciones que aumenten la seguridad de los activos de la organización.
- **Detección de Malware**: Hemos de mantener actualizado el antivirus con la última versión disponible, así protegeremos tanto el dispositivo como los recursos alojados en la nube.

- **Utilización de contraseñas robustas:** La renovación temporal de contraseñas y la condición de que estas sean robustas aumenta la seguridad, sobre todo en aquellos recursos que contengan información esencial.
- **Conexión segura:** Trabajemos siempre de forma segura, utilizando las redes VPN (Red Privada Virtual) proporcionadas por la organización para acceder a los recursos necesarios a la hora de desempeñar el trabajo.

Paquete de Seguridad Saas desde 18,5 € al año.

Desde **Grupo Oesía** consideramos esencial proteger a nuestros clientes y sus activos más esenciales. Por ello creemos que proteger el teletrabajo, hoy más que nunca, está justificado, contribuyendo de esta forma a la Continuidad de Negocio de nuestros clientes.

Características	Paquete de Seguridad SaaS
Paquete de Seguridad SaaS	
Protección ante amenazas de Día Cero	✔
Detección de Malware y uso de Sandbox (Detección de adjuntos maliciosos)	✔
Emulación de Amenazas	✔
Extracción de Amenazas	✔
Protección de email (Phishing, Spam, URL y otros)	✔
Protección de identidad	✔
Prevención de fuga de datos	✔
Descubrimiento SaaS Shadow IT	✔
Detección de anomalías	✔
Gestión intuitiva en la nube	✔
Aplicaciones Soportadas	
Office 365 mail	✔
OneDrive	✔
SharePoint	✔

Gmail	✔
Google Drive	✔
Salesforce	✔
Slack	✔
Box	✔
Dropbox	✔
Inteligencia de Amenazas	
Base de datos con amenazas CLOUD	✔
Gestión, Despliegue, Monitorización 24X7 y Gestión de Incidentes	
Gestión en la nube	✔

Contacte con nosotros
si quiere asegurar sus servicios en la nube:

cert@oesia.com

La seguridad de la información depende de ti.

Ciberseguridad | oesia

ciberseguridad.oesia.com