oesia
grupo

TELETRABAJO

Seguridad Móvil para la continuidad del negocio

2020

TELETRABAJO

La seguridad en el móvil para la continuidad del negocio

El uso de dispositivos móviles, tanto iOS como Android, facilita numerosas gestiones relacionadas con el trabajo y actividades derivadas de este, como la necesidad de contactar con compañeros, clientes, proveedores u otros.

Sin embargo, debemos ser conscientes de los riesgos y vulnerabilidades que pueden afectar al trabajo en remoto y en consecuencia a las compañías. Almacenamos y gestionamos grandes volúmenes de información en nuestros teléfonos o dispositivos móviles que, de llegar a las manos equivocadas, podrían suponer una amenaza directa a la empresa e incluso a nuestros clientes y proveedores. Tenemos constancia de que los cibercriminales aprovechan la confusión y la menor seguridad de nuestros dispositivos, para hacerse con dicha información y lograr sus objetivos.

Desde **Grupo Oesía** trabajamos para que el teletrabajo se realice de forma segura y, por ello, ofrecemos una **solución de seguridad complementaria para aumentar la seguridad de los dispositivos móviles de trabajo** y que todos los miembros de la organización puedan continuar con sus labores diarias con seguridad.

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

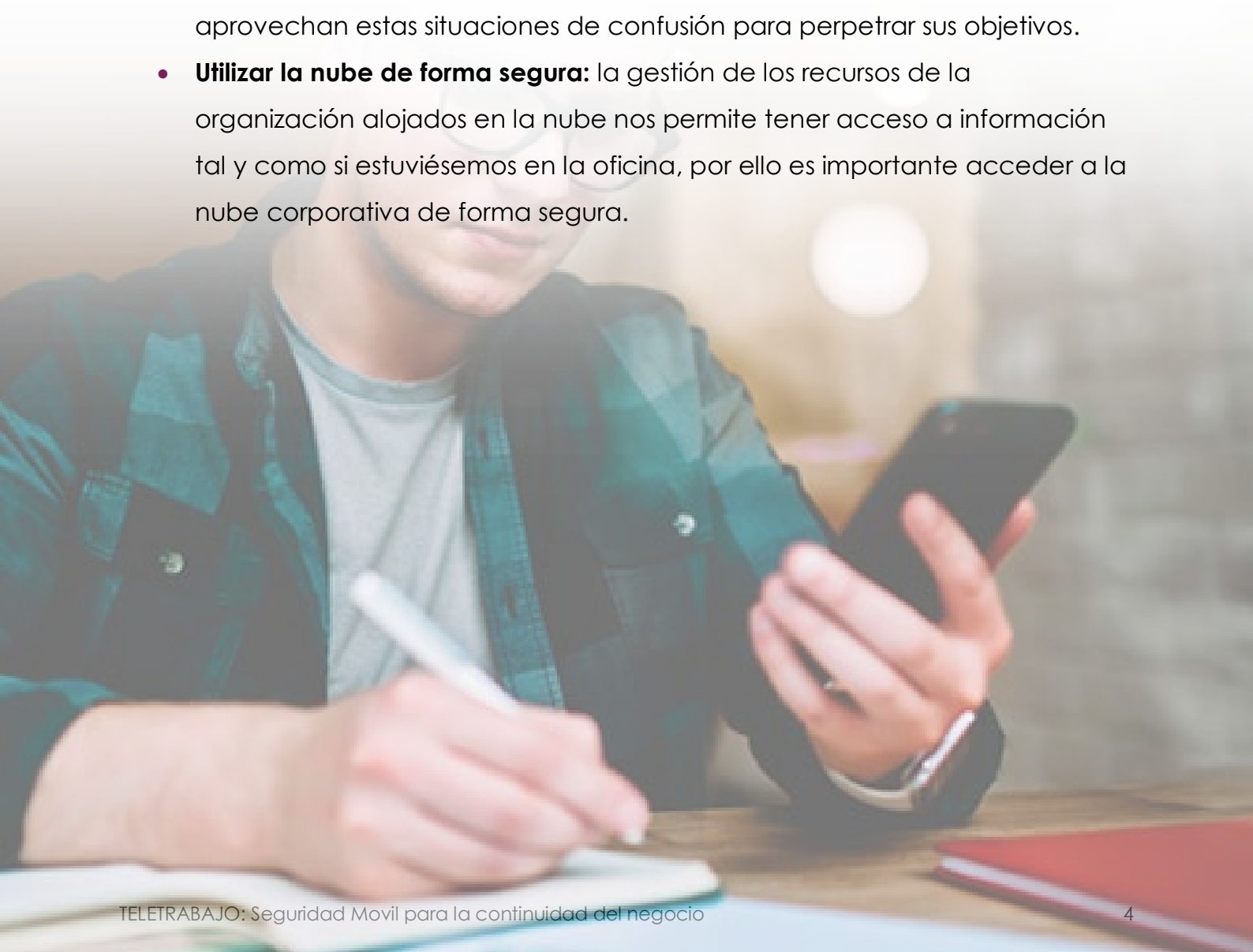
Retos a los que nos enfrentamos al teletrabajar con dispositivos móviles:

Al igual que exigimos cumplir la normativa y políticas de seguridad cuando trabajamos en las oficinas de la organización, debemos asegurar que cada profesional continúe aplicando estas medidas en su trabajo en remoto, a pesar de no disponer de los mismos recursos. Esta situación que nos exige la revisión de la normativa y políticas de seguridad, en relación al acceso remoto a las herramientas corporativas y la información que gestionamos, anticipándonos a la amenaza de los cibercriminales.

Estos puntos clave de seguridad se pueden resumir en 8 puntos clave:

- **Actualizaciones de seguridad:** mantener los dispositivos y aplicaciones del dispositivo actualizados tal y como nos advierten los fabricantes de software o sistema operativo es esencial para aumentar la seguridad en el teléfono móvil. Esta sencilla acción corrige las vulnerabilidades conocidas y mantiene seguro nuestro dispositivo y a la organización.
- **Aplicar los controles de seguridad**: el sistema operativo de los dispositivos móviles incluye controles de seguridad por defecto, que suelen ser modificados para ampliar funcionalidades. Hemos de aplicar dichos controles para tener un dispositivo seguro.
- **Utilizar exclusivamente redes inalámbricas seguras**: conectar nuestro dispositivo a redes inalámbricas públicas o inseguras pone en riesgo tanto el dispositivo como su información. La utilización de otro tipo de redes como Bluetooth o NFC también supone un riesgo para los activos de la organización. Hemos de asegurarnos que las redes con las que trabajamos son seguras y permiten que la información manejamos este a salvo.
- **Cifrar los dispositivos**: el valor de la información que contienen nuestros dispositivos de trabajo es incalculable y también esencial tanto para la realización de nuestras laborales como para la continuidad del negocio. Es importante cifrar todos nuestros dispositivos, incluyendo los de almacenamiento extraíble.

- **Instalar solo aplicaciones seguras:** instalemos exclusivamente aplicaciones necesarias para el trabajo. Hemos de evitar instalar aplicaciones de repositorios no seguros o aplicaciones que nos solicitan permisos no requeridos para la utilización de dicha aplicación.
- **Eludir la suplantación de identidad (Phishing):** debemos cuidar especialmente la comunicación electrónica que recibimos. Hemos de 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.
- **Proteger los 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.
- **Utilizar la nube de forma segura:** la gestión de los recursos de la organización alojados en la nube nos permite tener acceso a información tal y como si estuviésemos en la oficina, por ello es importante acceder a la nube corporativa de forma segura.



Paquete de Seguridad Móvil (iOS + Android)

desde 18,5 € al año por dispositivo.

Características	Sandblast Mobile
Análisis de Aplicaciones	
Detección de aplicaciones maliciosas conocidas y desconocidas	✔
Emulación de Amenazas	✔
Análisis de código estático avanzado	✔
Reputación de aplicaciones	✔
Machine Learning	✔
Prevención de Malware	✔
Evaluación de Dispositivos	
Evaluación de riesgos en tiempo real	✔
Detección de ataques	✔
Detección de vulnerabilidades	✔
Detección de cambios en la configuración	✔
Detección avanzada de Rooting y Jailbreaking	✔
Detección de dispositivos comprometidos	✔
Prevención de Ataques basados en Red	
Prevención de ataques de Phishing	✔
Prevención de robo de credenciales	✔
Prevención de ataques Man-in-the-Middle	✔
Prevención de comunicación con servidores de comando y control (C&C)	✔
Prevención de sitios web y URL maliciosas	✔
Remediación dinámica de Amenazas	
Bloqueo de acceso a aplicaciones y datos corporativos	✔

Remedio de amenazas	✔
Remediación y Contención	
Bloqueo de tráfico a servidores de comando y control (C&C)	✔
Prevención de movimientos laterales y aislamiento de máquinas infectadas	✔
Finalización de proceso y cuarentena de archivos	✔
Restauración de archivos encriptados	✔
Esterilización completa de la cadena de ataque	✔
Inteligencia de Amenazas	
Base de datos de 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