PRESIDENCIA DE LA REPÚBLICA DOMINICANA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

GUIA SOBRE DISPOSITIVOS MÓVILES PARA USO PROFESIONAL

DISPOSITIVOS MÓVILES PARA USO PROFESIONAL

La expansión de la utilidad de dispositivos móviles, la mejora en las conexiones y en elementos de hardware han generado un cambio significativo en la forma de trabajar, utilizando el internet para mantenerse conectado todo el tiempo en cualquier lugar. Cada día las empresas están más orientadas a implementar soluciones que permitan el acceso a sus recursos y a la información.

Este nuevo escenario laboral trae consigo una nueva complejidad, ya que tenemos dispositivos personales con acceso a informaciones, y a recursos de la empresa, al tiempo que la red corporativa es utilizada para fines privados.

Esto conlleva una serie de riesgos importantes para la seguridad de las ompañías como, por ejemplo:

- Pérdida de información.
- Robo de dispositivos o de credenciales e instalación de aplicaciones personales que podría comprometer la confidencialidad de la información corporativa.
- Responsabilidad por daños a terceros.

Es por ello que debemos establecer políticas y mecanismos adecuados de seguridad para los dispositivos móviles personales ara implementar la gestión, y políticas internas que implanten configuraciones de seguridad específicas y adaptar los dispositivos personales a las medidas de seguridad corporativas existentes.

En este documento se describen los requisitos fundamentales de seguridad exigidos para los dispositivos móviles con el objetivo de aplicar la mínima seguridad que cualquier producto de esta familia debe tener. Estos requisitos incluyen mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas.

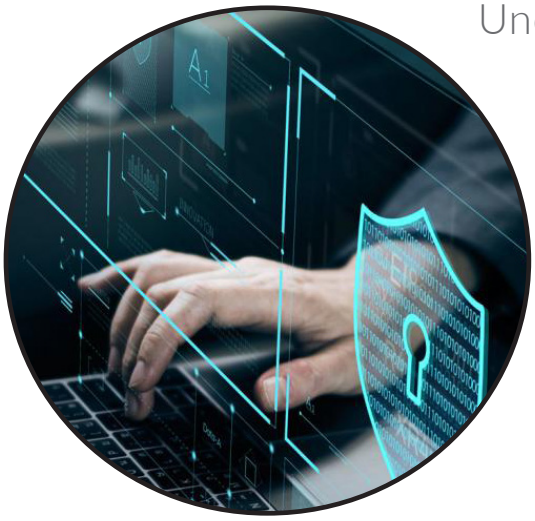
Medidas de seguridad

Los dispositivos móviles tanto, para uso personal como laboral deben estar protegidos convenientemente, mediante medidas de seguridad apropiadas que ayuden a reducir todo lo posible los riesgos expuestos. Para incorporar estas medidas se pueden utilizar herramientas específicas que gestionan dispositivos móviles. En el mercado existen soluciones, de este tipo que sirven para administrar y monitorear los dispositivos móviles, permitiendo controlar los dispositivos y valorar el grado que se encuentran implementadas las medidas de nuestra política de seguridad.

Con estas herramientas es posible gestionar y controlar:

- los dispositivos autorizados para acceder a aplicaciones y recursos;
- las aplicaciones instaladas en los dispositivos;
- las configuraciones de seguridad del dispositivo, de su wifi y su VPN;
- las manipulaciones indebidas de los terminales como la detección de jailbreak en iOS o rooteo en Android;

- el bloqueo remoto de dispositivos extraviados;
- la destrucción/formateo remoto de datos de dispositivos extraviados o robados el cifrado de datos o del dispositivo, y
- la detección de malware la fortaleza y renovación de contraseñas.



Uno de los puntos fundamentales es involucrar al usuario y concienciarlo sobre el uso correcto de los dispositivos. Sin su colaboración las medidas no van a ser efectivas, ya que el usuario es quien gestiona la información. Un empleado comprometido, que cumpla las normas y políticas de seguridad de la empresa, evitará los riesgos sobre la pérdida de control sobre la gestión de los dispositivos.

Protección de la información

La información generada en la empresa es su activo más importante, por lo que deben tomarse medidas sobre los siguientes puntos:

1- aplicaciones instaladas;
2- almacenamiento en la nube;
3- cifrado de dispositivo;
4- copias de seguridad, y
5- almacenamiento local de data empresarial.

Aplicaciones instaladas

Al momento de diseñar las políticas de uso de aplicaciones debemos tomar en cuenta que muchas de estas aplicaciones requieren permisos a otras aplicaciones o datos que deben ser gestionado con atención. como por ejemplo las que solicitan acceso a información de teléfono, contacto, videos, fotos, correo electrónico, etc. Todo esto puede provocar que se pierda el control de la actividad del dispositivo y nuestros datos.

Al momento de instalar aplicaciones se deben realizar las siguientes acciones:

- descargar e instalar únicamente las que se encuentran permitidas por la empresa;
- leer siempre las condiciones de uso e instalación para controlar los permisos de acceso, y
- descargar las aplicaciones de las tiendas oficiales para evitar instalación de malware.

Almacenamiento en la Nube

Se debe tener especial cuidado con la forma de acceso y almacenamiento de los datos corporativos en los dispositivos móviles personales, especialmente a la hora de utilizar aplicaciones de intercambio de archivos.

Para garantizar la seguridad de la información se deberán utilizar únicamente los servicios en la nube autorizados por la empresa. Antes de utilizar estos servicios debemos tomar en cuenta:

- las condiciones de uso en lo referente a las garantías de disponibilidad y confidencialidad de la información;
- las posibles restricciones del proveedor respecto al tipo de datos que podemos almacenar;
- dónde acudir en caso de fallo del servicio, medidas de protección de la información o los tiempos de indisponibilidad permitidos por contrato;
- ll tipo y frecuencia con la que el proveedor realiza las copias de seguridad de sus servidores.

Otros aspectos a tomar en cuenta son:

- implementar la necesidad de contraseñas para el acceso directo a los datos en los servicios;
- establecer acuerdos de nivel de servicio con los proveedores que suelen incluir penalizaciones en caso de incumplimiento, e

- instrumentar mecanismos de cifrado y el acceso mediante autenticación en los dispositivos móviles;

Copias de seguridad

Las copias de seguridad son una medida común en las empresas, pero tambien es muy común olvidarse de incluir los dispositivos móviles personales de uso corporativo en las políticas de respaldos.

Esta medida no nos protege de los ataques a los que estaríamos expuestos debido a los riesgos que generan los dispositivos móviles, pero nos garantiza que podremos recuperar rápidamente la información importante si el dispositivo se vuelve inaccesible, si la terminal se pierde o es robada, si hay un fallo de material o un borrado inadvertido , entre otros.

Al momento de realizar copias de seguridad debemos tener en cuenta las siguientes medidas:

- las copias se deben almacenar fuera del dispositivo,
- en recursos de la empresa y, en caso de contener información personal, se deberán tomar las medidas correspondientes para proteger la información;

- realizar las copias de forma automática cada cierto tiempo;

- el fijar el número y periodicidad de estas según las necesidades propias de cada empresa,
- debe existir la posibilidad de hacer copias de manera manual, en caso de que el sistema automático falle, y
- se debe corroborar que se están realizando las copias de seguridad y realizar pruebas de restauración para verificar el correcto funcionamiento de las mismas.

Cifrado de dispositivos

Ya sea por pérdida, robo o cualquier otro motivo, los dispositivos de información tienen un gran riesgo y de verse comprometidos, la confidencialidad de la información puede verse afectada por el acceso no autorizado. Con la implantación de sistemas de cifrado se transforma la información de tal forma que solamente aquellas personas que estén autorizadas puedan leerla o manipularla.

Todos los sistemas actuales permiten habilitar opciones de cifrado de datos y dispositivos mediante contraseñas de acceso o a nivel de arranque.

Configuración de dispositivos

Para minimizar los riesgos derivados del robo de las credenciales de acceso o de la desaparición de los dispositivos eben tomarse una serie de medidas técnicas que aseguren la integridad de los dispositivos.

Por ello, configuraremos los terminales con una serie de funcionalidades que nos ayudarán a mantener la confidencialidad de la información:

- instalar y configurar un antivirus;
- configurar las actualizaciones del software;
- habilitar la autenticación robusta y de doble factor para las aplicaciones críticas;
- desactivar la opción de recordar contraseñas, y
- configurar el cifrado de datos y comunicaciones;

Localización remota

En caso de pérdida de dispositivos la localización remota proporciona funcionalidades efectivas:

- localización de las terminales, ya que el dispositivo envía información de su ubicación mediante GPS, WIFI, entre otros medios;
- bloqueo remoto del terminal, para evitar el uso del dispositivo por personas no autorizadas;
- borrado remoto, de los datos contenidos en el dispositivo, y
- seguimiento de actividad del dispositivo para vigilar las aplicaciones que están siendo ejecutadas.

Es importante saber que estas aplicaciones permiten realizar un seguimiento profundo del dispositivo por lo que su utilización debe quedar restringida a causas justificadas, ya que puede implicar la violación a la privacidad del usuario, en caso de robo, las informaciones obtenidas deben ser puestas a disposición de las autoridades para fines de investigación.

Geolocalización

Los dispositivos móviles permiten habilitar de forma selectiva el geoposicionamiento según las preferencias del usuario. Es recomendable mantener deshabilitado esta funcionalidad siempre que no sea estrictamente necesaria. Al momento de instalar aplicaciones hay que prestar atención a las que solicitan acceso al posicionamiento del dispositivo y permitirlo solo cuando sea necesario. En el caso de las empresas, esta puede ser una información importante para recuperar el dispositivo en caso de pérdida.

En cualquier situación, el uso de este servicio puede implicar la violación de la privacidad del usuario, por lo cual, antes de activarlo debe y firmarse un acuerdo de consentimiento.

Protección de conexiones a redes externas

Es importante identificar mecanismos para asegurar la confidencialidad de los datos en las comunicaciones realizadas entre los dispositivos móviles y los recursos centralizados cuando se haga uso de redes ajenas a la empresa que no sean seguras.

También es importante ser precavidos en lugares públicos donde habrán personas a nuestro alrededor que pueden observar cómo introducimos nuestras credenciales.

Redes wifi y redes privadas virtuales (VPN)

Al momento que se requiera conectar a una red que no garantice la seguridad se deberán buscar mecanismos para que la comunicación se realice con la mayor seguridad posible.

Para hacer más segura la conexión a una red desprotegida y evitar el robo de credenciales y manipulación de nuestra información personal, de trabajo, etc., debemos establecer las siguientes medidas:

- desconfiar de redes WiFi públicas y gratuitas.
- utilizar canales de cifrado seguro de comunicación o algún otro tipo de cifrado punto a punto;
- desconectar la wifi de los dispositivos cuando no se esté utilizando;
- desactivar la conexión automática a redes.
- hacer uso, preferentemente, de redes 3G y 4G antes que WiFi.

Estas medidas son válidas para todo tipo de dispositivo y casos de uso.

Si necesitas realizar acceso mediante una red no segura, crear canales seguros cifrados de comunicación garantiza la confidencialidad de la información. Las redes privadas virtuales (VPN) crean un túnel a través de internet de forma que protege la transferencia de información y la conexión a los recursos de la empresa únicamente de los dispositivos aprobados.

CASOS DE USO

Dispositivo propiedad de la empresa para uso corporativo general y para uso personal limitado.

En este caso la entidad ejerce un cierto control sobre la configuración y el software del dispositivo.
Para uso de correo corporativo, acceso a VPN, entre otras tareas.

Dispositivo propiedad de la empresa para uso corporativo de ALTA seguridad.

La entidad se autoexige un alto control sobre la configuración y el software limitado para manejar o utilizar información sensible. Se conectará a la red corporativa para acceder a servicios corporativos en caso que las políticas lo permitan.

Dispositivo propiedad del empleado para uso personal y corporativo , también conocido como Bring Your Own Device (BYOD).

La organización provee al dispositivo con recursos necesarios para lograr acceso a la red corporativa y los servicios que ofrece e implementar controles de seguridad para mitigar los posibles incidentes que puedan reproducirse.