Universidad Veracruzana

Seguridad en Dispositivos Móviles

Ciberseguridad
UV-CSIRT

Información segura... ¡es cultura!®

Seguridad en Dispositivos Móviles

Hoy en día cada vez es más frecuente la necesidad de utilizar soluciones tecnológicas a través de dispositivos móviles en las empresas e instituciones que ayudan a facilitar el acceso a la información de la misma desde cualquier parte. Sin embargo, trabajar con estos dispositivos conlleva importantes riesgos en la seguridad de la información.

Riesgos en el uso de dispositivos móviles

Pérdida o robo de información

Mal uso que se pueda hacer de los dispositivos

Robo de dispositivos

Robo de credenciales (usuario y password)

Conexión a redes inseguras

Los datos de GPS pueden ser muy útiles para ciertas tareas, pero permiten a otros saber dónde nos encontramos en cada momento.

Configuraciones inseguras.

Considerando estos riesgos y las amenazas cibernéticas que existen actualmente, es fundamental que todos los usuarios que hagan uso de dispositivos móviles para realizar distintas funciones y que gestionen información institucional, sigan las siguientes medidas de seguridad en los dispositivos móviles.

Medidas de seguridad para la protección de la información en dispositivos móviles

• **Establecer el bloqueo de pantalla de forma automática.** Es una práctica que debemos realizar, debido a que un bloqueo automático de pantalla ayudará a evitar que alguien no autorizado acceda a nuestro teléfono.

Seguridad en Dispositivos Móviles

• **Protege el acceso al dispositivo.** Se debe establecer medidas de autenticación seguras del usuario, para ello es importante definir un patrón, una contraseña o un desbloqueo por algún sistema biométrico.

• **Usar doble factor de autenticación:** Para los servicios o aplicación que gestionen información sensible, siempre que sea posible, se recomienda habilitar un segundo factor de autenticación.

• **Mantener el sistema operativo y apps actualizados.** Permite minimizar los riesgos de ser víctimas de un incidente de seguridad, ya sea por una mala configuración del dispositivo o por una vulnerabilidad en el software.

• **Realizar configuraciones seguras.** Limitar los permisos de las apps, es decir no dar permisos innecesarios a las apps, para limitar así los datos y funcionalidad a la que tendrán acceso, limitar lo máximo posible la funcionalidad disponible en la pantalla de bloqueo.

• **Nunca dejar un dispositivo móvil o portátil desatendido.** Un dispositivo no controlado es un dispositivo vulnerable. Se deben tener controlados y localizados en todo momento.

• **Descargar aplicaciones únicamente de fuentes fiables.** Si es necesario instalar una nueva aplicación, lo mejor es descargarla de tiendas oficiales. No hacerlo puede poner en peligro la información e integridad del dispositivo.

• **Utilizar siempre que sea posible una conexión segura.** En la conexión remota a la red de la institución, establecer siempre conexión por VPN para proteger las comunicaciones. Esto evitará que la información transmitida sea comprometida. También hay que prescindir de conectarse a redes inalámbricas abiertas o no confiables, ya que no siempre estas se configuran de forma segura, así como limitar el uso de bluetooth cuando no sea necesario.

• **Prevenir ataques phishing.** Al recibir correos electrónicos, mensajes de texto, desconfiar de aquellos que lleven archivos adjuntos o enlaces sospechosos, que provengan de desconocidos, que no hayan sido solicitados, o tengan un sentido de urgencia.

• **Navegación segura.** Siempre que sea posible, ingresar a sitios web que cuenten con certificados de seguridad, es decir mediante https:// antes de introducir la dirección web del servidor con el que se desea conectar. Sin embargo, nunca se debe aceptar un mensaje de error del navegador web que esté relacionado al certificado inválido, recomendándose la cancelación de la conexión.

Seguridad en Dispositivos Móviles

• **Realizar copias de seguridad de la información.** Respaldar los datos almacenados en el dispositivo de forma periódica permitirá que la información siempre se tenga disponible ante la pérdida o robo del dispositivo.

• **Cifrar la información.** El cifrado de los datos es fundamental para proteger la información institucional almacenada en el dispositivo como la que se envía a través de mensajería instantánea, correo electrónico, etc.

Los dispositivos móviles de forma nativa tienen capacidades de cifrado que podrán utilizarse estableciendo un código de acceso robusto ya que éste será utilizado en el proceso de cifrado.

Algunos dispositivos móviles IOS activan de manera automática las capacidades de cifrado una vez que se establece un código de acceso.

En el caso de dispositivos móviles Android más recientes, las capacidades de cifrado también están activas de forma automática. Sin embargo, en caso de tener una memoria externa se puede cifrar también la información.

• **Habilitar el acceso y el borrado de datos en remoto.** Utilizar herramientas que faciliten el bloqueo y borrado de la información institucional o personal en caso de robo o pérdida del dispositivo.

• **No conectarse a puertos USB desconocidos** y no realizar alguna transferencia de archivos confidenciales a través de USB en lugares públicos, por ejemplo restaurant, ya que no se tiene certeza de estar conectado a un equipo de confianza.

La concientización, el sentido común y las buenas prácticas en la configuración y uso de los dispositivos móviles son la mejor defensa para proteger la información de las amenazas cibernéticas.

Normatividad de la Universidad Veracruzana

La Universidad Veracruzana cuenta con un Reglamento de Seguridad de la Información que establece las responsabilidades de los usuarios con el uso adecuado de los recursos de TI que la Universidad le brinda, no cumplir con las medidas de control para la seguridad de la información física o lógica establecida en el mismo podría ser causa de sanción en los términos de la legislación universitaria y las leyes aplicables en la materia.

Seguridad en Dispositivos Móviles

Referencias

https://www.incibe.es/protege-tu-empresa/blog/incorporacion-segura-dispositivos-moviles-empresa
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf
https://angeles.ccn-cert.cni.es/index.php/es/docman/documentos-publicos/informes-de-buenas-practicas/297-ccn-cert-bp-03-dispositivos-moviles/file
https://www.uv.mx/legislacion/files/2019/12/Seguridad-de-la-Informacion-2019-Gaceta.pdf