Recomendaciones en el uso de dispositivos fuera de entornos controlados durante los desplazamientos

Abstract: en este documento se recogen una serie de recomendaciones y buenas prácticas para el uso seguro de dispositivos electrónicos fuera de entornos controlados e instalaciones propias de una organización. La aplicación de las siguientes medidas contribuye a la reducción de la superficie de exposición ante cualquier posible ataque.

Contenido:

1. INTRODUCCIÓN 1
2. ANTES DEL DESPLAZAMIENTO 2
   2.1 Control de la información 2
   2.2 Mejoras de seguridad en los dispositivos 2
3. DURANTE EL DESPLAZAMIENTO 3
   3.1 Limitar el acceso físico de terceros a los dispositivos 3
   3.2 Conexiones 4
   3.3 Protección de datos 4
   3.4 Correo electrónico 5
   3.5 Navegación web 5
4. DESPUÉS DEL DESPLAZAMIENTO 7

1. INTRODUCCIÓN

En el desplazamiento fuera de entornos controlados e instalaciones propias de una organización, se recomienda ser especialmente prudente con los dispositivos electrónicos (portátiles, tabletas, teléfonos móviles y memorias USB), tanto por el valor de la información que contienen (personal y laboral) como por sus características físicas. Además, la portabilidad de estos dispositivos les convierte en objetivos relativamente fáciles de sustraer, especialmente en lugares concurridos como aeropuertos, hoteles, restaurantes, conferencias, etc. donde aumenta la probabilidad de que sean extraviados o robados.

Por otro lado, la facilidad de conexión de los dispositivos móviles a redes de comunicaciones con distinto nivel y requisitos de seguridad, como por ejemplo redes *Wi-Fi* públicas abiertas, aumenta el riesgo de sufrir ataques y de infección de los propios dispositivos.

Las recomendaciones que se detallan a continuación, en la medida en que se apliquen, contribuirán a reducir la superficie de exposición ante cualquier posible ataque. En los siguientes epígrafes se indican una serie de buenas prácticas, clasificadas en función de los momentos del desplazamiento.

2. ANTES DEL DESPLAZAMIENTO

2.1 Control de la información

a. Una vez identificada y seleccionada la información sensible, que es imprescindible durante el desplazamiento, es preferible almacenarla en un dispositivo que no vaya a estar conectado a redes de comunicaciones y que no se utilice para navegar por Internet. Además, se debe mantener una copia de seguridad de la misma en un dispositivo que permanezca en las instalaciones propias.

b. Se aconseja no llevar dispositivos extraíbles (tipo memorias USB o tarjetas SD) ya que, por su tamaño, es fácil extraviarlos o que sean sustraídos sin tener una constancia inmediata. Si se considerase necesarios portarlos, se debería evitar que contuvieran información de interés.

c. En cualquier caso, los dispositivos removibles (discos duros externos, memorias USB, tarjetas SD, etc.) que almacenen información sensible deben ir cifrados.

d. El cifrado de los discos duros en los equipos portátiles constituye una medida de seguridad para impedir el acceso no autorizado a la información. Dependiendo del sistema operativo existen aplicaciones propietarias con este propósito y, en su defecto, las particiones con información sensible estarán cifradas mediante aplicaciones ex profeso para tal fin.

e. En los dispositivos móviles existe una funcionalidad, incluida en el sistema operativo dentro de los ajustes de seguridad, que permite cifrar todo el almacenamiento y que exige definir una contraseña de bloqueo de pantalla para el dispositivo.

f. Siempre que sea posible, se debe eliminar la documentación sensible (personal y laboral) de los dispositivos electrónicos. Se recomienda utilizar herramientas de borrado seguro.

2.2 Mejoras de seguridad en los dispositivos

a. Definir contraseña de bloqueo de pantalla. Preferiblemente deberá ser alfanumérica, teniendo en cuenta que cuanto más compleja sea, mayor será la dificultad de acceso no autorizado.

b. Actualizar, a la última versión disponible, el sistema operativo del dispositivo y las aplicaciones instaladas, especialmente las concernidas con la seguridad como el antimalware.

c. En los ordenadores portátiles, el usuario no debe disponer de permisos de “Administrador”. Asimismo, se debe tener instalada una solución antivirus y configurado un cortafuegos personal que restrinja al menos las comunicaciones

entrantes y filtre las salientes (el cortafuegos integrado en el sistema operativo puede resolver de manera adecuada este punto).

d. Con el objetivo de prevenir alteraciones en el sistema de arranque o el acceso a la información cuando un atacante tiene acceso físico al equipo, es recomendable revisar y activar los mecanismos de protección BIOS/UEFI y gestores de arranque del dispositivo. La protección de arranque UEFI de los equipos más modernos ayuda a proteger el sistema contra *rootkits*[1] y otras formas de ataque por medios removibles.

e. En dispositivos móviles y tabletas se recomienda desinstalar aplicaciones no utilizadas. En el caso de aquellas aplicaciones instaladas por el fabricante, que no se utilicen y que no se puedan desinstalar, se recomienda al menos inhabilitarlas con el objetivo de limitar su ejecución en segundo plano y la realización de conexiones a Internet no deseadas.

f. Se insta a instalar una aplicación VPN[2] para proteger las conexiones realizadas. Se aconseja llevar a cabo esta recomendación antes de realizar el desplazamiento por si existiese alguna restricción de descarga o dificultad de instalación durante el mismo.

g. Cuando no se disponga de una VPN corporativa, o de un servicio de *proxy* en la nube, y la conexión no sea a un servicio cifrado, se recomienda utilizar un servicio de VPN donde no se asocie la navegación al usuario o un método de pago. En este sentido, convendría valorar la posibilidad de emplear versiones gratuitas donde el tráfico y conectividades relacionadas pueden pasar más desapercibidas o incluso, considerar la utilización de conexiones a través de la red *Tor*[3].

IMPORTANTE: se han de revisar y configurar todos los dispositivos electrónicos que se vayan a utilizar durante el desplazamiento, intentando llevar lo imprescindible y minimizar la exposición a la amenaza.

3. DURANTE EL DESPLAZAMIENTO

3.1 Limitar el acceso físico de terceros a los dispositivos

a. Se ha de definir una contraseña de bloqueo de pantalla, especialmente en aquellos dispositivos que no siempre acompañen al usuario. En el caso de que queden desatendidos, es preferible dejar los dispositivos encendidos con la pantalla

[1] *Rootkits* es un conjunto de herramientas usadas frecuentemente por atacantes que consiguen acceder ilícitamente a un sistema informático.
[2] VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar uno o más dispositivos a una red privada utilizando Internet.
[3] Se debe evaluar el balance de riesgos entre utilizar una red como *Tor*, que limita el poder identificar la conexión original, frente a establecer conexiones dónde se pueda trazar por un tercero la navegación del usuario o un método de pago.

bloqueada para detectar más fácilmente si alguien ha intentado manipularlos (por ejemplo, modificar la ROM).

b. Si el dispositivo lo permite, utilizar métodos de identificación biométrica (huella dactilar o detección facial).

c. Evitar el uso de tarjetas SD en dispositivos móviles, pues son fácilmente extraíbles.

d. No realizar conexiones (USB, Bluetooth, NFC[4], etc.) con dispositivos no confiables. Se evitará conectar medios extraíbles a los dispositivos que contengan información sensible, sobre todo si dichos medios han sido entregados por personas no confiables.

3.2 Conexiones

a. La implementación del doble factor de autenticación (2FA) es crucial para usuarios remotos.

b. Desactivar funcionalidades no necesarias, especialmente en dispositivos móviles y tabletas: Bluetooth, NFC, conexión Wi-Fi compartida y localización. Además, se deberán modificar los parámetros establecidos por defecto en la configuración.

c. Desactivar la conexión de datos (Wi-Fi y 3/4G) siempre que no se esté utilizando.

d. Evitar la conexión a redes Wi-Fi abiertas (aeropuerto, centros comerciales, …) y, en general, no confiables.

e. Utilizar la funcionalidad que algunos sistemas operativos incorporan de utilizar una dirección física privada para contribuir a reducir el seguimiento del dispositivo cuando se conecta a diferentes redes Wi-Fi.

f. Se recomienda, en la medida de lo posible, evitar el uso de comunicaciones inalámbricas, empleando alternativas cableadas como las redes Ethernet. Si fuese necesario utilizar una conexión de datos, los mecanismos recomendados son:

   - Conexión *3/4G* en *roaming*, que no siempre es posible por restricciones de presupuesto.
   - Conexiones *Wi-Fi* confiables y túnel VPN para cifrar las conexiones.

3.3 Protección de datos

a. En caso de detectar cualquier ataque o comportamiento anómalo durante el desplazamiento, se debe comunicar al responsable de seguridad TIC del Organismo.

[4] NFC (Near-Field Communication) es una tecnología inalámbrica de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos.

b. Evitar acceder a aplicaciones corporativas (correo electrónico, bases de datos, etc.) si no se está utilizando una comunicación cifrada para ello, como puede ser una VPN.

c. No instalar aplicaciones de origen desconocido. En los dispositivos móviles solo se deben instalar las aplicaciones procedentes de mercados (*markets*) oficiales; en los ordenadores portátiles, sólo aquellas aplicaciones cuyo origen sea confiable.

d. En la medida de lo posible, se recomienda no utilizar el mismo dispositivo para navegar por Internet y para el tratamiento de información sensible y/o conexión a servicios corporativos. En este sentido, la utilización de máquinas virtuales para la conexión a Internet favorece la compartimentación.

3.4 Correo electrónico

a. El correo electrónico constituye uno de los vectores de infección más habituales hoy en día. La concienciación, el sentido común y las buenas prácticas en el uso del correo electrónico son las mejores defensas para prevenir y detectar incidencias.

b. Se recomienda ser especialmente cuidadoso con los correos electrónicos recibidos; se debe comprobar que la dirección del remitente (nombre y dominio) es conocida y confiable. De no ser así, no se debería abrir el correo.

c. No abrir ningún enlace ni descargar ningún fichero procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo considerado normal o habitual.

d. Antes de abrir cualquier fichero descargado desde el correo, asegúrese de comprobar la extensión del mismo.

e. Se debe evitar hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, se recomienda buscar primero información en motores de búsqueda como Google o Bing antes de acceder al mismo.

f. No habilitar la ejecución de macros en los documentos ofimáticos descargados, aunque el propio fichero lo solicite.

g. Si existiese necesidad de enviar información sensible por correo electrónico, se debe cifrar el mensaje y/o adjuntos.

3.5 Navegación web

a. Uno de los métodos de infección más utilizados es la explotación de vulnerabilidades en los navegadores web. Por ello, posiblemente una de las pautas más importantes que debe seguirse es asegurarse de que el navegador, así como *plugins* y extensiones, están actualizados a su última versión.

b. Se recomienda el uso de máquinas virtuales para la navegación por Internet. De esta forma, se favorece el aislamiento entre los entornos que habitualmente realiza cualquier usuario que teletrabaja:
   - Acceso a Internet.
   - Consumo de la información corporativa.

c. Si su sistema operativo lo permite, como alternativa a la máquina virtual, se recomienda habilitar la protección de aplicaciones, la cual permite ejecutar el proceso de la aplicación en un contenedor aislado.

d. Revisar las opciones de seguridad y privacidad del navegador: no aceptar *cookies* de terceros, bloquear *pop-ups*, usar solamente TLS 1.2 y superior (bloquear SSL, TLS 1.0 y TLS 1.1), evitar la sincronización de contraseñas, evitar autocompletado, borrar ficheros temporales y *cookies* al cerrar el navegador, bloquear la geolocalización, filtrar *ActiveX*, etc.

e. Si se navega por páginas desconocidas es recomendable que el usuario deshabilite *plugins* como *Flash/Java* e incluso *JavaScript*.

f. Para navegar por Internet, se debe utilizar un usuario sin permisos de "Administrador", así se disminuye la superficie de exposición al limitar la instalación de programas y cambios en la configuración del sistema operativo.

g. Acceder únicamente a sitios web de confianza.

h. Se debe evitar acceder a páginas web en las que se muestre un aviso de certificado digital inválido. En este caso, es mejor cancelar la conexión.

i. Es preferible no almacenar las contraseñas de acceso a aplicaciones en el propio navegador web ya que éstas pueden ser recuperadas en caso de infección por código malicioso.

j. Configurar el sistema operativo para forzar el uso de proveedores DNS seguros, que incluyan filtros de sitios maliciosos, contenido inapropiado o potencialmente dañino.

La información anterior se puede ampliar con las guías de buenas prácticas de correo electrónico, navegadores web y dispositivos móviles disponibles en el Portal web del CCN-CERT (https://ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp.html).

IMPORTANTE: intentar no dejar "desatendidos" los dispositivos electrónicos y no conectarse a ninguna red o página web no confiable. En caso de detectar alguna incidencia o comportamiento anómalo durante el desplazamiento, se debe comunicar con la mayor brevedad al responsable de seguridad TIC del Organismo.

4. DESPUÉS DEL DESPLAZAMIENTO

a. Si existe la más mínima duda de haber sido víctima de un ciberataque, no se han de conectar los dispositivos electrónicos a la red corporativa. Como mínimo es recomendable ejecutar un análisis antivirus y en casos más extremos puede ser necesario llevar a cabo un análisis forense o incluso una restauración de la imagen (o reseteo a valores de fábrica) del equipo.

b. No es aconsejable conectar a la red corporativa los dispositivos removibles (memorias USB) entregados por terceros sin revisión y aprobación previa del responsable de seguridad TIC del Organismo.

c. Informar con la mayor brevedad al Departamento TIC de los problemas e incidencias detectadas para que puedan ser analizadas de cara a próximos desplazamientos.

IMPORTANTE: siempre que exista alguna sospecha, se deberá solicitar un análisis forense del equipo susceptible de haber sido atacado y se evitará conectar a la red corporativa los dispositivos removibles recibidos como obsequio.

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.01.17 11:31:21 +01'00'