RECOMENDACIONES PARA EL USO DE DISPOSITIVOS MÓVILES

Riesgos y protección

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

UNIVERSIDAD DE SEVILLA

crue Universidades Españolas

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
www.incibe.es

ÍNDICE

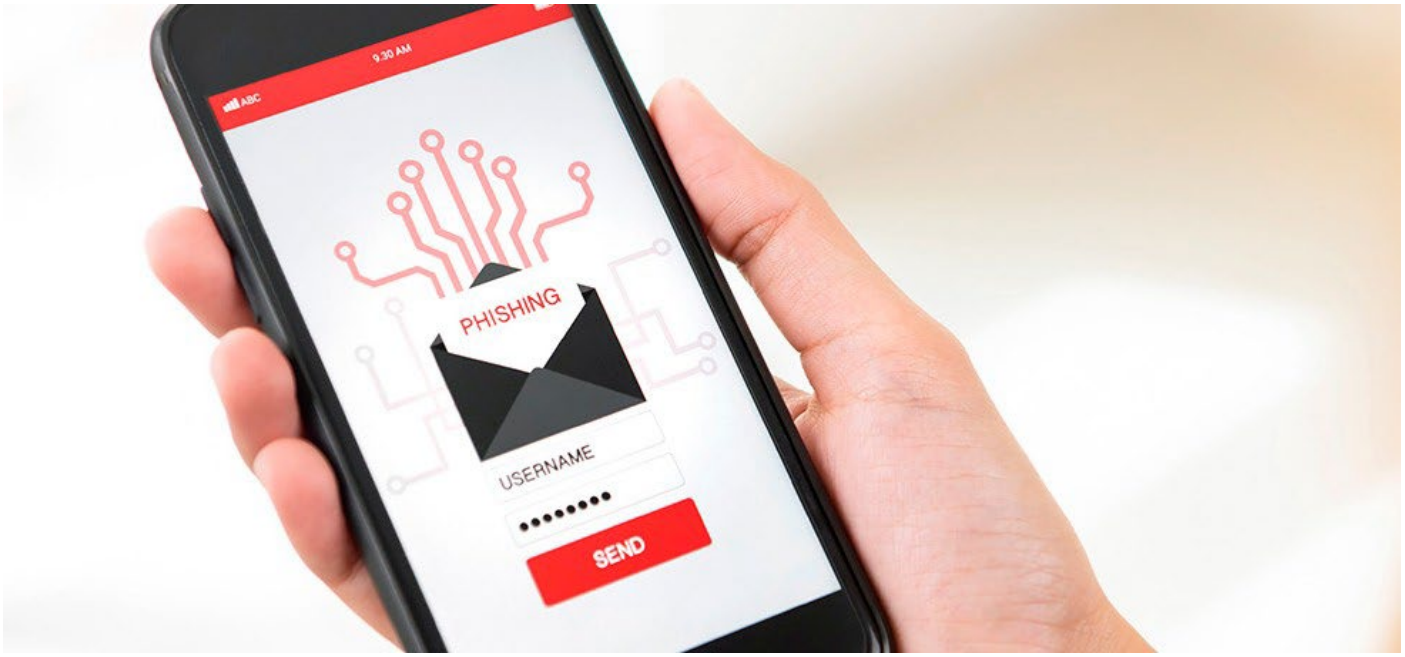
1. RECOMENDACIONES PARA EL USO DE DISPOSITIVOS MÓVILES

Consultar el correo, acceder a una hoja de cálculo o hacer una modificación a última hora de un documento importante, desde cualquier lugar, son solo algunas de las tareas que se pueden llevar a cabo desde los dispositivos móviles **[Ref. - 1**]. En la actualidad, estos aparatos se han convertido en herramientas imprescindibles para el trabajo o el estudio, gracias a su movilidad y su conexión a Internet.

Ordenadores portátiles, smartphones o tablets permiten a la comunidad universitaria desempeñar su trabajo o estudio en cualquier sitio, como si estuviera en las instalaciones de la universidad, lo que ha abierto un abanico nuevo de posibilidades, pero también nuevos riesgos para la universidad que los propios usuarios deben tener en cuenta.

2. RIESGOS ASOCIADOS

Los dispositivos móviles, tabletas y portátiles debido a su reducido tamaño y a la capacidad que tienen de gestionar información de la empresa, entrañan nuevos riesgos. También en el teletrabajo, además de utilizar dispositivos móviles, nos conectamos desde el exterior de la red de la universidad, utilizamos servicios para compartir documentos y contamos con riesgos asociados a entornos de trabajo no tan controlados.



Estos son los principales riesgos asociados a los dispositivos móviles y al teletrabajo:

- **El robo o pérdida** de los móviles, tabletas, portátiles y dispositivos de almacenamiento como discos duros externos y pendrives. Este puede ser el riesgo más importante al que se exponen estos dispositivos debido a su tamaño y en muchos casos, a su elevado coste.

- **La infección por malware** siempre es un riesgo a tener en cuenta, pues el software malicioso puede robar información confidencial de la empresa y credenciales de acceso a diferentes recursos. A menudo descuidamos la protección antimalware en equipos pequeños.

- **Los sitios web fraudulentos**, la publicidad agresiva o las páginas web de tipo phishing son las principales amenazas a las que se exponen. Navegar en dispositivos pequeños, particularmente en móviles, entraña riesgos al ser más difícil «librarse» de esta publicidad.

- **Utilizar redes wifi inseguras** puede poner en riesgo la privacidad de las comunicaciones, ya que los ciberdelincuentes pueden estar «escuchando» todo lo que se envía y recibe. También podemos conectarnos a redes wifi que suplantan a redes wifi lícitas.

2. RIESGOS ASOCIADOS

- **Instalar aplicaciones** que necesitan acceder a determinados permisos del dispositivo, en ocasiones excesivos o innecesarios (como acceso a la cámara, los contactos o los archivos), para poder funcionar con normalidad, pudiendo así verse la información empresarial comprometida.

- Dispositivos que **no cuentan con controles de acceso robustos** que los protejan de un descuido, robo o pérdida. La ausencia de los mismos o el uso de algunos considerados débiles, como el patrón de bloqueo, son un riesgo para su seguridad.

- Tanto el **sistema operativo, como las aplicaciones desactualizadas** suponen un riesgo para la seguridad de toda la información que gestionan.

- **La modificación de los controles de seguridad impuestos por los fabricantes.** Algunos usuarios deciden rootear o hacen jailbreak a sus dispositivos, lo que puede suponer un grave riesgo, ya que los controles de seguridad impuestos por el desarrollador son eliminados.

- **Establecer que el dispositivo o la aplicación recuerde la contraseña.** Si un tercero accede al dispositivo tendría acceso a todos los servicios en los que estuviera guardada la contraseña.

- **Utilización de servicios en la nube.** La utilización de servicios en la nube o cloud puede suponer un riesgo, ya que la información de la empresa será almacenada en un tercero al que hemos de trasladar nuestros requisitos de confidencialidad, integridad y privacidad. Además, existe el riesgo de que si no fuera posible conectarse a Internet (problemas en la red como congestión o caída de la misma) la información almacenada en la nube no será accesible.

3. MEDIDAS DE PROTECCIÓN

Para contrarrestar los riesgos mencionados, la comunidad universitaria debe aplicar las siguientes medidas de protección.

3.1. Protección antimalware y sitios web peligrosos

Las infecciones causadas por cualquier tipo de malware, siempre están presentes. Todo tipo de códigos maliciosos pueden llegar por correo electrónico y mensajería, en pendrives, a través del navegador o de aplicaciones. Además de entrenarnos para detectar enlaces y ficheros sospechosos, navegar de forma segura y descargar aplicaciones fiables, es importante disponer de **herramientas [Ref. - 2] que detecten y eliminen el software malicioso.** Por otra parte, los sistemas **antivirus siempre deberán estar actualizados** a la última versión, algo que propiciará la identificación del malware más actual.

Es común que los antivirus también cuenten con herramientas que permitan **identificar posibles sitios web fraudulentos o peligrosos,** como aquellos utilizados para cometer phishing. Al seleccionar un antivirus para el móvil verificaremos que disponga de estas funcionalidades.

3.2. Protección contra accesos no autorizados

Para evitar que terceros sin permiso accedan a toda la información que gestiona el dispositivo es necesario implantar una serie de controles:

- **Contraseña de firmware,** si el dispositivo lo permite, sobre todo en ordenadores portátiles. De esta forma, se evita que otros usuarios arranquen el equipo desde otro disco distinto del especificado.

- **Creación de cuentas de usuario y permisos.** En los sistemas operativos como Windows, MacOS o los basados en Linux, se permite la creación de distintos usuarios, otorgándoles una serie de privilegios acordes con su perfil. Es recomendable que **cada usuario cuente con los privilegios mínimos y necesarios que le permitan desempeñar su trabajo**. Además, deberán contar con una **contraseña de acceso robusta.**

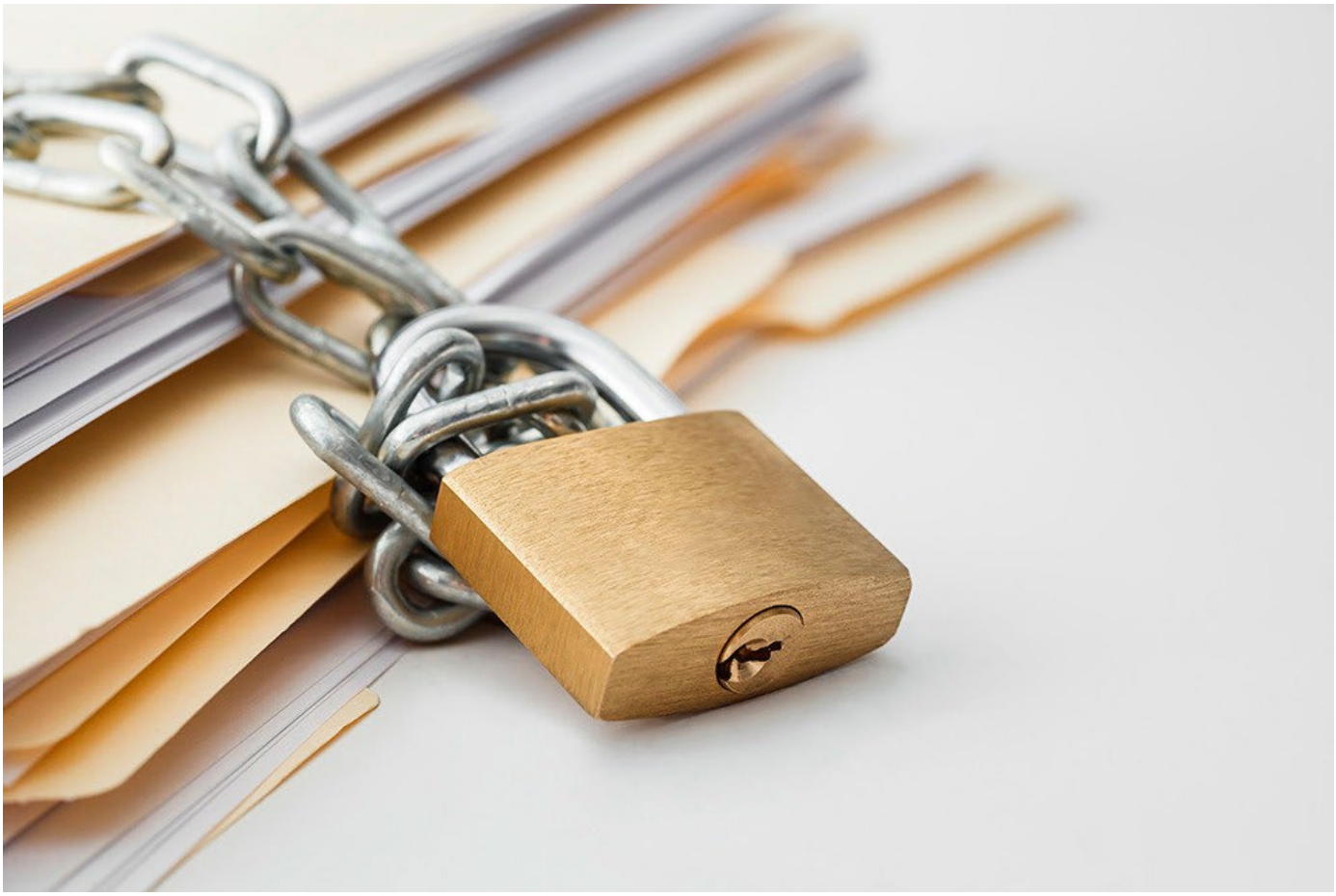
- **Bloqueo de dispositivos.** En los dispositivos basados en Android o iOS hay que establecer el **bloqueo de pantalla en el menor tiempo posible y una contraseña de desbloqueo robusta.** También pueden utilizarse métodos biométricos como la huella dactilar.

3.3. Protección de la información

La información que se gestiona desde los dispositivos móviles o portátiles que se utilizan para el trabajo o estudio diario puede ser de gran importancia, por lo que protegerla será prioritario. Para ello, se recomienda seguir las siguientes recomendaciones:

- **Activar el cifrado de la información en el dispositivo.** Todos los sistemas operativos deberán contar con herramientas de cifrado que protejan la información en ellos alojada. Los actuales sistemas operativos móviles como Android e iOS cuentan con cifrado de la información por defecto, pero los sistemas operativos para ordenador no, por lo que se debe activar.

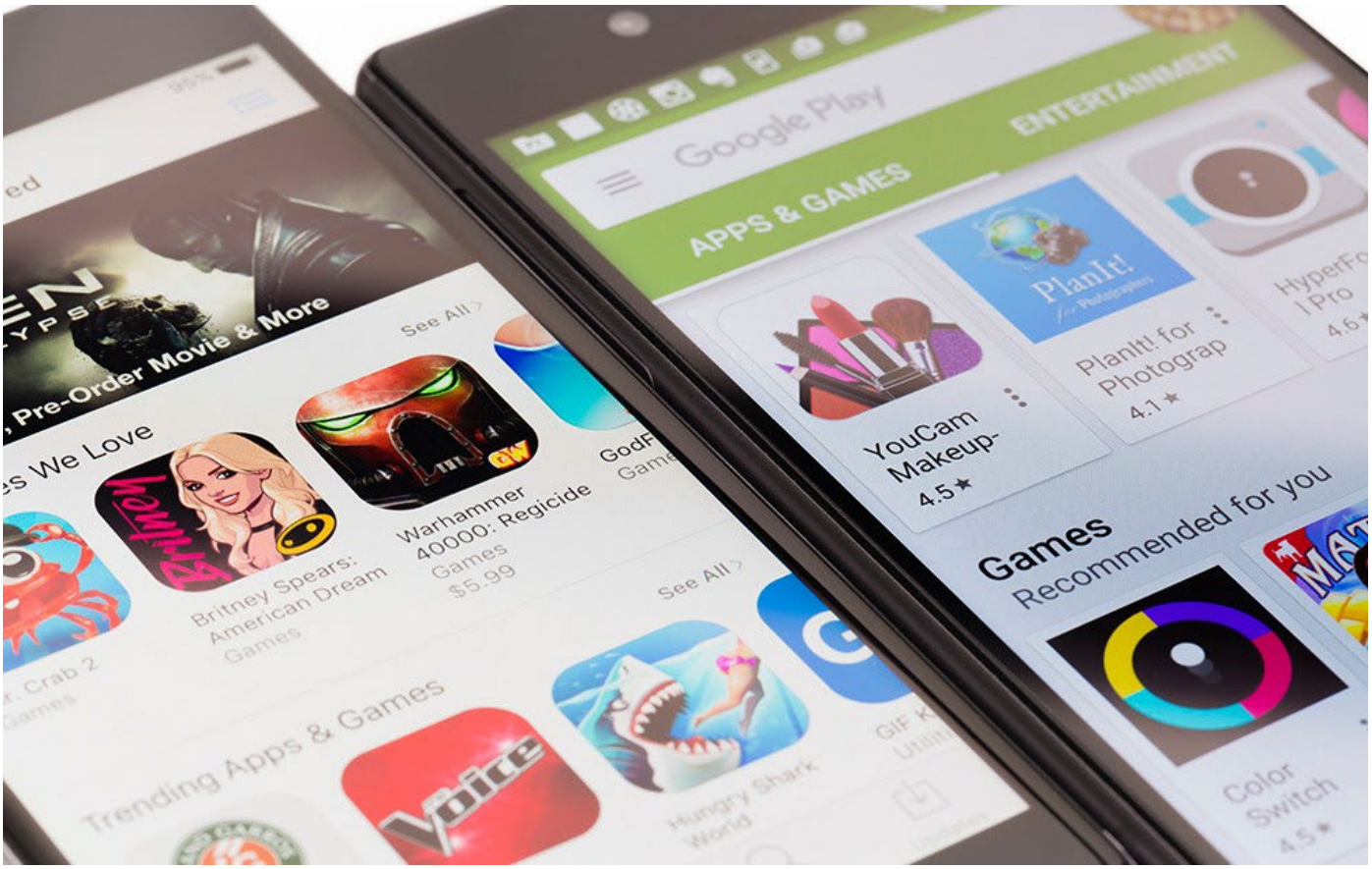
- **Establecer cuál será el tratamiento aceptable de la información confidencial.** En el caso del personal de administración y servicios de la universidad, investigadores y docentes, se accederá preferiblemente a la misma por medio de Internet y se evitará siempre descargar en el dispositivo.



3.4. Aplicaciones legítimas

Las aplicaciones para dispositivos móviles **deben ser descargadas, únicamente, desde la tienda oficial.** Para teléfonos inteligentes y tabletas estas deben ser descargadas **desde la App Store para Apple o desde Play Store para Android.** En caso de ordenadores, como ya se indicó anteriormente, deben ser descargas desde el sitio weboficial.

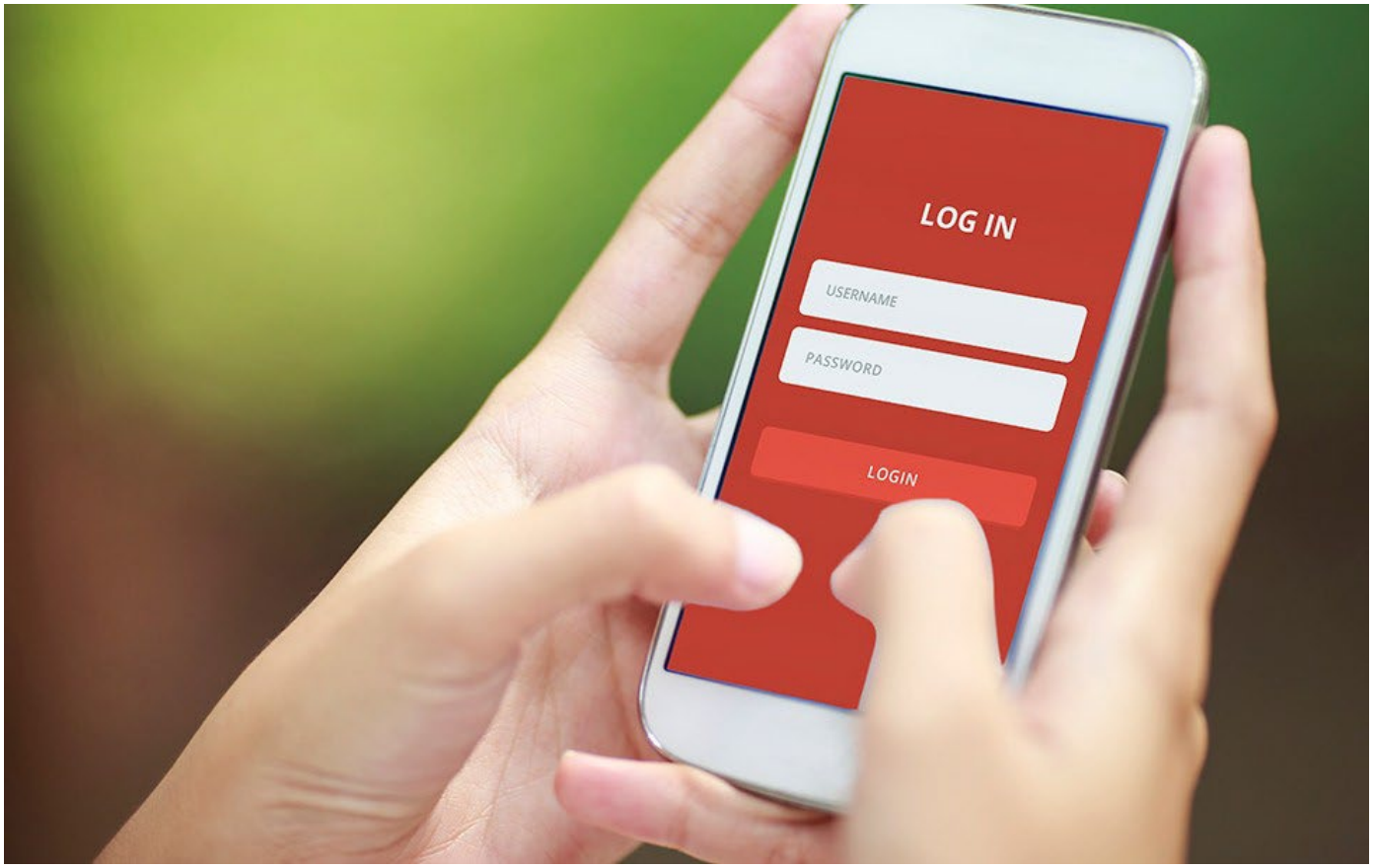
La universidad deberá proveer de software legítimo, es decir, deberá estar en posesión de una licencia válida, en caso contrario estaría incurriendo en un delito. Todo el software utilizado y sistemas operativos estarán **actualizados** a la última versión disponible, además de que será siempre descargado de **fuentes legítimas** y contará con las debidas **licencias de uso.**



3.5. No recordar la contraseña

La función de **«Recordar contraseña» no debe usarse nunca en dispositivos móviles,** ya que ante un acceso no autorizado se podría acceder a todos los servicios donde se haya activado esta función.

En caso de utilizar múltiples servicios, con múltiples contraseñas, es recomendable utilizar un gestor de contraseñas que ayude en esa tarea.



3.6. No utilizar redes wifi inseguras

Con frecuencia nos encontramos en distintos establecimientos y servicios públicos que ofrecen conexión wifi de manera gratuita a sus clientes. A pesar del ahorro que pueda suponernos, **no es recomendable utilizar estas conexiones wifi** que nos encontramos en hoteles, restaurantes, estaciones de tren, aeropuertos, etc., ya que no conocemos su seguridad, ni su legitimidad (podrían fácilmente haberlas suplantado) y la privacidad de la información que enviamos o recibimos puede verse comprometida.

Siempre es mejor opción utilizar la conectividad móvil 4G que incorporan los dispositivos (conexión de datos), especialmente cuando se realizan tareas sensibles como acceder a banca online o a información que pueda ser confidencial.

En el caso del personal de administración y servicios, docentes e investigadores para los que sea habitual viajar por motivos de trabajo y sea necesario disponer de conectividad, se ha de **utilizar una VPN [Ref. - 3]** (red privada virtual) que cifre las conexiones extremo a extremo, para acceder a los recursos necesarios. Se evitará, en la medida de lo posible, utilizar aplicaciones de escritorio remoto para conectarse a servidores de la universidad sin VPN.

3.7. Otras medidas de protección en caso de estudio o trabajo online

En ocasiones, las tareas a realizar se tienen que trasladar al hogar **[Ref. - 8]**. Seguir manteniendo un aceptable nivel de ciberseguridad es igualmente vital, siendo necesario tomar, además del uso de aplicaciones legítimas, contraseñas, bloqueo del equipo y cifrado de información confidencial, las siguientes medidas:

- no se permitirán usos domésticos (juegos, descargas, etc.) por otros usuarios en el dispositivo utilizado como puesto de trabajo o estudio;
- se realizarán **copias de seguridad** de forma periódica;
- en caso de utilizar una **conexión wifi doméstica** que podamos configurar de forma segura **[Ref. - 9]** tendremos encuenta:
  - utilizar cifrado WPA2 o WPA3 en caso de estar disponible y que los dispositivos sean compatibles;
  - utilizar una clave robusta;
  - desactivar la función WPS en caso de estar activa.

4. ¿QUÉ ES EL BYOD?

El uso de dispositivos personales como ordenadores portátiles, smartphones o tablets, propiedad del empleado de la universidad, ya sea personal de administración y servicios, docentes o investigadores, para realizar sus tareas laborales, es lo que se conoce como BYOD **[Ref. - 4]** del inglés *Bring Your Own Device.* Se trata de una práctica muy frecuente que beneficia tanto a la universidad, reduciendo costes, como al empleado, permitiéndole una mejor conciliación laboral, o en el caso del estudiante, una mayor flexibilidad para el estudio.

A pesar de los beneficios que aporta, son varios los riesgos que su uso conlleva, por lo que se debe prestar especial atención para que su uso no comprometa la seguridad de la información personal o de la universidad.

4.1. Principales riesgos

Además de los riesgos mencionados para el uso de dispositivos móviles hay que añadir algunos que son exclusivos **[Ref. - 5]** del BYOD como:

- **Distracciones de los empleados.** Al utilizar un mismo dispositivo para tareas personales, laborales o de estudio, la productividad puede disminuir al acceder a páginas web no relacionadas con su actividad profesional, redes sociales o la cuenta privada de correo electrónico.

- **Aumento de las posibilidades de accesos no autorizados** a información sensible de la universidad, ya que el dispositivo se usa para trabajar y para uso personal. Por lo tanto, las posibilidades de pérdida o robo aumentan y, por consiguiente, también aumentan los accesos no autorizados.

- El **dispositivo puede ser prestado** a un amigo o familiar para realizar cualquier tarea, lo que puede poner en riesgo la seguridad de la información personal o de la universidad.

- La **relación contractual entre el empleado y la universidad puede llegar a su fin** pudiendo ser un riesgo para ambas partes conservar información de la institución una vez ha terminado el contrato.

4.2. Medidas de seguridad a tomar

Al ser dispositivos donde los usuarios de la universidad tienen un mayor control sobre ellos, las medidas complementarias **[Ref. - 6]** a las anteriormente indicadas son:

- **No realizar modificaciones en el software del dispositivo.** Los dispositivos Android e iOS cuentan con restricciones de fábrica que aumentan su seguridad y la de la información que manejan. Nunca hay que hacer Jailbreak o rootear un smartphone.
- **El dispositivo se mantendrá siempre bajo custodia**, incluso ante amigos y familiares.
- Desde la universidad, en el caso de BYOD para trabajadores propios, se debe elaborar una **normativa** que regule el uso de estos dispositivos, el registro de dispositivos y aplicaciones autorizadas, las configuraciones de seguridad a aplicar, si será necesaria la localización por GPS, canales de comunicación seguros, etc.

5. ¿QUÉ HACER EN CASO DE ROBO O PÉRDIDA DEL DISPOSITIVO?

La pérdida o el robo es el principal incidente de seguridad que afecta a estos dispositivos, por lo tanto, se debe tener un plan B para que la información de la universidad, y la personal en caso de ser BYOD, no se vean afectadas.

Los pasos a seguir son:

- **Ponerlo en conocimiento de la institución** para que se tomen todas las medidas necesarias que eviten el uso indebido del dispositivo y de la información que contiene o a la que tiene acceso.

- Si el dispositivo ha sido robado, se deberá **interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado [Ref. - 7],** aportando toda la información posible.

- **Bloquear el dispositivo de manera remota.** La mayoría de sistemas operativos tanto para ordenador, como para móvil cuentan con herramientas que lo permiten, generalmente a través de un panel de administración web.

- **Geolocalizar el dispositivo.** Actualmente, los dispositivos con sistema operativo Windows, MacOS, Android e iOS cuentan con herramientas que permiten conocer su posicionamiento aproximado. Siempre que sea necesario se debe tener habilitado en dispositivos que use el empleado. La universidad tiene que avisar a los empleados de forma clara, expresa e inequívoca, tal y como indica la LOPDGDD3/2018.

- En caso de no ser posible recuperar el dispositivo, se debe optar por **realizar un borrado remoto del mismo**, de tal manera que toda la información que contenga no pueda estar accesible. Para ello, tendremos habilitada esta opción.

6. REFERENCIAS

1. INCIBE – Protege tu empresa – Herramientas – Políticas de seguridad - Uso de dispositivos móviles corporativos - https://www.incibe.es/protege-tu-empresa/blog/dia-mundial-las-contrasenas-aun-utilizas-123456

2. INCIBE – Protege tu empresa – Blog – Descubre cómo proteger tu empresa del malware - https://www.incibe.es/protege-tu-empresa/blog/descubre-proteger-tu-empresa-del-malware

3. INCIBE – Protege tu empresa – Blog - Conéctate a tu empresa de forma segura desde cualquier sitio con una VPN - https://www.incibe.es/protege-tu-empresa/blog/conectate-tu-empresa-forma-segura-cualquier-sitio-vpn

4. INCIBE – Protege tu empresa – Herramientas – Políticas de seguridad - Uso de dispositivos móviles no corporativos - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-no-corporativos.pdf

5. INCIBE – Protege tu empresa – Blog - Bondades y riesgos del BYOD - https://www.incibe.es/protege-tu-empresa/blog/bondades-y-riesgos-del-byod

6. INCIBE – Protege tu empresa – Blog - ¿Trabajas desde tu dispositivo móvil? ¡Implementa las mismas medidas de seguridad que en tu oficina! - https://www.incibe.es/protege-tu-empresa/blog/trabajas-tu-dispositivo-movil-implementa-las-mismas-medidas-seguridad-tu

7. INCIBE – Protege tu empresa – Reporte de fraude - https://www.incibe.es/protege-tu-empresa/reporte-fraude

8. INCIBE – Protege tu empresa – Blog - ¿Tu casa también es tu oficina? ¡Protégela! - https://www.incibe.es/protege-tu-empresa/blog/tu-casa-tambien-tu-oficina-protegela

9. INCIBE – Protege tu empresa – Guías - Seguridad en redes wifi: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario