UAEM

EL PUESTO DE TRABAJO

Medidas de protección I

meta red

DTIC

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

www.incibe.es

www.incibe.es

ÍNDICE

1. IMPORTANCIA DE PROTEGER EL PUESTO DE TRABAJO

El puesto de trabajo es el lugar en el que realizamos nuestras tareas diarias en la universidad. Como parte de estas actividades cotidianas, cualquier usuario requiere acceder a diversos sistemas y manipular diferentes tipos de información. Como consecuencia directa, debemos tener en cuenta que **el puesto de trabajo es clave desde un punto de vista de la seguridad de la información [Ref. - 1].**

Son varios los riesgos a los que se expone el puesto de trabajo:

- información en papel al alcance de cualquiera;
- la falta de confidencialidad de los medios de comunicación tradicionales como el teléfono;
- accesos no autorizados a los dispositivos;
- infecciones por malware;
- robo de información;
- etc.

Por ello, es necesario que apliquemos un conjunto de medidas de seguridad que nos garanticen que la información, tanto en papel como en formato electrónico, está correctamente protegida.

2. BUENAS PRÁCTICAS

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la universidad, se deben seguir buenas prácticas para proteger el puesto de trabajo.

2.1. Mesas limpias

En el día a día de la universidad es habitual trabajar con distintos documentos en papel que se dejan encima de la mesa para mayor comodidad o porque son necesarios para las tareas diarias.

Sin embargo, **al acabar la jornada se debe guardar la documentación que se encuentre a la vista** (información de la universidad, estudiantes, profesores, etc.). Esto es especialmente importante si se trabaja en entornos compartidos. De esta manera, se evitarán miradas indiscretas que puedan derivar en una fuga de información, además del robo de documentos que pueden contener información confidencial.

Se debe prestar especial atención a que:

- el puesto de trabajo esté limpio y ordenado;
- la documentación que no se utilice en un momento determinado debe estar guardada correctamente, especialmente cuando se abandona el puesto de trabajo o se finaliza la jornada;
- no haya usuarios ni contraseñas apuntadas en post-it o similares.

Además, también tendremos que guardar fuera del alcance de terceros, cuando no estemos en nuestro puesto, los dispositivos informáticos que se puedan desconectar, como USB o discos duros.

2.2. Bloqueo de sesión

Cuantas veces nos hemos levantado de nuestro puesto de trabajo y no hemos bloqueado el equipo, incluso cuando estábamos trabajando en un documento muy importante. ¿Y si alguien hubiera accedido al equipo y hubiera copiado el documento, o si hubiera enviado un correo electrónico haciéndose pasar por quien no es? Todas esas situaciones y otras muchas se pueden evitar con un simple bloqueo de sesión.

Los dispositivos, como ordenadores, tablets o móviles, con los que se esté trabajando siempre deben estar bloqueados, a no ser que se esté en presencia de ellos.

En dispositivos de sobremesa y ordenadores portátiles, el bloqueo de pantalla se realiza por medio de los siguientes atajos de teclado:

- Windows: Win + L
- MacOS: Control + Opción + Q
- Linux: Control + Alt + L

En dispositivos móviles como smartphones o tablets se ha de establecer el bloqueo de pantalla en el menor tiempo posible y preferiblemente por contraseña o biométrico, como la huella dactilar, siempre sin interceder en la actividad laboral.

También es posible que programemos en los distintos sistemas, con ayuda del soporte informático, si fuera necesario, un bloqueo automático de sesión en caso de inactividad, para que si no se detecta actividad pasado este tiempo, se bloquee el dispositivo.

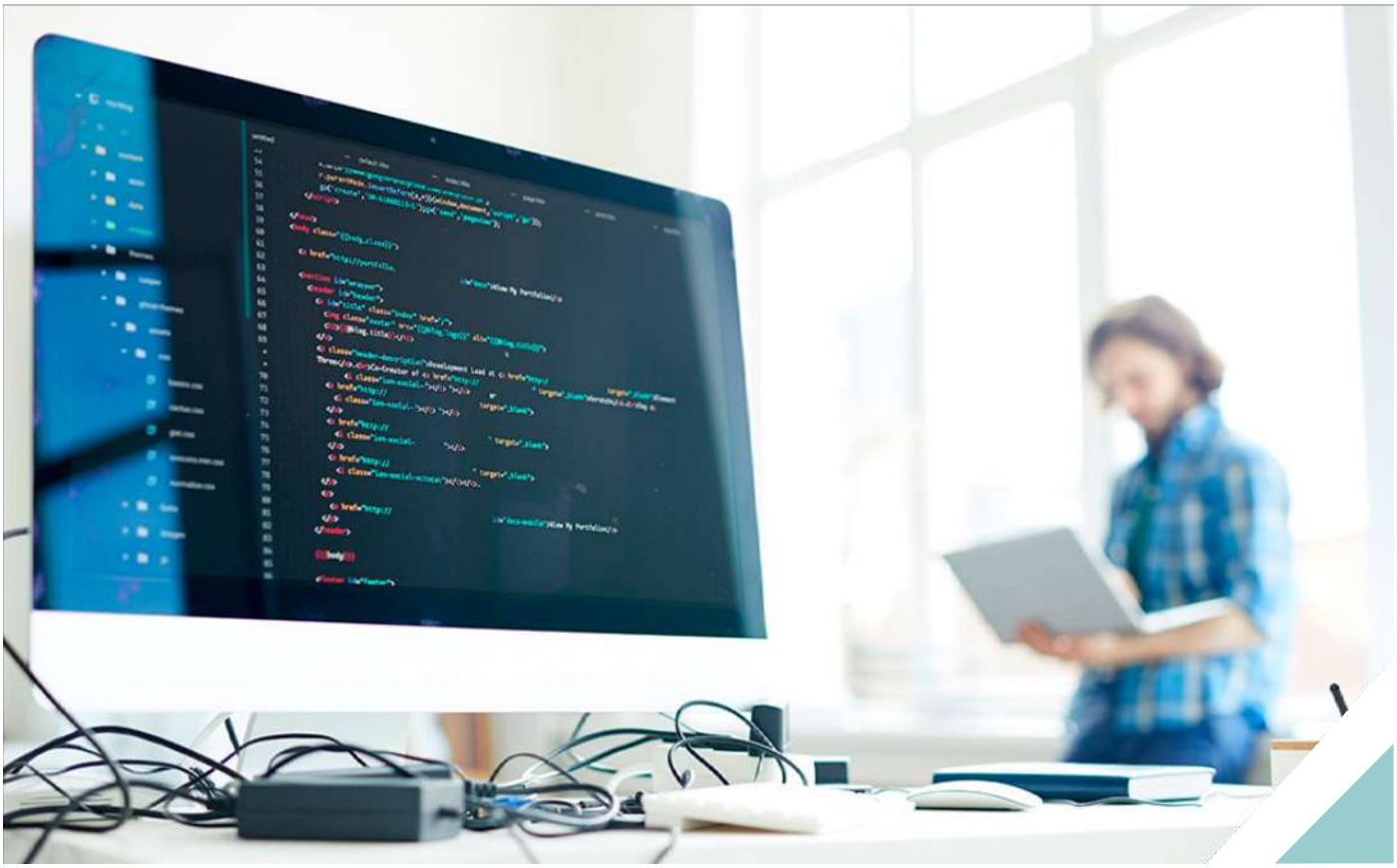
Y, al terminar la jornada, dejaremos siempre los equipos apagados y si fueran portátiles o móviles, bajo llave.

2.3. Software actualizado

Todos los sistemas de la empresa deben estar actualizados a la última versión disponible, de esta manera estarán protegidos ante nuevas vulnerabilidades descubiertas y contarán con las últimas funcionalidades que haya liberado el fabricante.

Para que todos los dispositivos estén siempre actualizados es recomendable habilitar las actualizaciones automáticas, tanto en el sistema operativo como en las distintas herramientas que tengan instaladas y que dispongan de esta opción.

Un dispositivo desactualizado es un riesgo para la seguridad de la empresa, ya que un ciberdelincuente puede aprovecharse de vulnerabilidades no parcheadas para acceder a la información de la empresa.



2.4. Antivirus y firewall

Tanto el antivirus [Ref. - 3] como el firewall o cortafuegos son las herramientas de seguridad que protegen al equipo del software malicioso. Ambas herramientas siempre deben estar activadas, ya que son complementarias, es decir, las tareas que realiza el antivirus no interfieren con las del cortafuegos y viceversa.

El antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso, también conocido como malware. Actualmente, incorporan otras herramientas de seguridad como detección de webs fraudulentas o protección contra ransomware.

El firewall o cortafuegos tienen el objetivo de permitir y limitar, el flujo de tráfico que va desde y hacia Internet evitando así que el malware pueda comunicarse con el exterior y que ataques procedentes de Internet sean bloqueados.

Como con cualquier tipo de software, ambas herramientas deben estar configuradas y actualizadas a la última versión, ya que así detectarán un mayor número de amenazas.

3. REFERENCIAS

1. INCIBE – Protege tu empresa – Herramientas - Políticas de seguridad para la pyme - Protección del puesto de trabajo. Políticas de seguridad para la pyme - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-puesto-trabajo.pdf

2. INCIBE – Protege tu empresa - ¿Qué te interesa? - Protección del puesto de trabajo - https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-puesto-trabajo

3. INCIBE – Protege tu empresa – Blog - ¿Qué hace un antivirus para detectar el malware? - https://www.incibe.es/protege-tu-empresa/blog/hace-antivirus-detectar-el-malware