PLAN DE SEGURIDAD INFORMÁTICA EOI DE CEUTA
CURSO 2018-19

1. JUSTIFICACIÓN

Ante el riesgo de un ciberataque se hace necesario hoy en día realizar un plan de seguridad informática por dos motivos: el primero, detectar vulnerabilidades con el fin de prevenir ciberataques tales como el robo de datos, virus como el ramsonware (programas que encriptan el disco duro y piden un rescate), creación de contraseñas seguras, protección de ordenadores, etc. El segundo motivo es tener claro una línea de actuación en el caso de que haya sucedido un problema relacionado con la seguridad informática, como, por ejemplo, cómo actuar si tu ordenador se ha infectado con un virus, si sospechamos que ha habido una intrusión en nuestro correo electrónico, o si perdemos el teléfono móvil.

Este plan de seguridad es breve de forma consciente para que todos los docentes tengan un acceso básico y rápido a la información. Estará colgado en los departamentos y estará incluido en el plan TIC.

Por último, hay que ser consciente de que la seguridad absoluta no existe, pero que, sin embargo, hay que tratar de adoptar medidas para evitar en lo posible la pérdida o robo de datos y el fraude.

2. ORDENADORES

2.1. SEGURIDAD PASIVA

Todos los ordenadores de la EOI están provistos de antivirus (Mc Affee, con subscrición, o bien AVG) y antimalware (Malwarebytes), además del Firewall de Windows.

El docente debe hacer un escaneado completo de su equipo con ambos programas una vez al mes. El profesor TIC realizará esto una vez al año, en junio.

MUY IMPORTANTE

- Los docentes tendrán el menor privilegio posible en los ordenadores y se establecerán cuentas personales a cada profesor, sin derechos de administrador. El administrador será el profesor TIC. No te asustes, lógicamente cederá derechos si algún profesor lo necesita en algún momento determinado.
- No descargues nunca programas de páginas como Taringa o uptodown, o de servidores que no sean los directos del producto. Por ejemplo, descargar el navegador Chrome de una página que no sea la de Chrome. Muchas veces es como el caballo de Troya, que trae regalo.
- Actualiza, actualiza, actualiza todo el software.
- Elige buenas contraseñas y siempre una para cada cosa. Ten en cuenta que no es lo mismo un programa de educación simple, que Facebook o la aplicación del banco. Es verdad que la seguridad es incómoda, pero ahí va un truco: piensa en una frase sencilla, que te sea fácil de recordar, y le haces una pequeña modificación, por ejemplo, las “oes” las cambias a “ceros”, las “ies” a “unos”.

Un ejemplo, si tienes un perro al que quieres mucho: *Quiero a mi perrito*. Quedaría: *Qu1er0amiperr1t0*. Un programa de fuerza bruta (que descifra contraseñas) tardaría varios años en descifrar el ejemplo.

Deberías cambiar las contraseñas (por lo menos las más importantes) al menos una vez al año.

- Mucho cuidado con los correos con archivos adjuntos, sobre todo si son de origen desconocido. Bórralos sin pinchar en ellos.
- Evita en lo posible el uso de una unidad USB, es una fuente importante de infecciones. Fíjate que los ordenadores que más problemas han dado con infecciones han sido el del laboratorio, y el de la biblioteca, que curiosamente, son los que más gente utiliza. Puedes utilizar nubes como Google Drive, u otras que hay en el mercado (Drop Box, One Drive, iCloud, etc)

2.2 SEGURIDAD ACTIVA

Si tienes dudas razonables de que tu ordenador ha sido infectado por un virus, pásale inmediatamente el antivirus y el antimalware, y en caso de encontrar algo ponlo en cuarentena o elimínalo, y comunícalo a tu profesor TIC.

3. DATOS

- Realiza copias de seguridad. Es la última y mejor línea de defensa ante la pérdida de datos valiosos. Deberías hacer una copia de seguridad al menos una vez al año. Esto es muy poco, hay quien hace copias de seguridad cada semana. Lo debes hacer en el disco duro cifrado del departamento. También puedes considerar la nube, pero como complemento y no como reemplazo.
- Si tienes información valiosa, debe estar cifrada (nombre, dirección, teléfonos de los alumnos). Tú eres el responsable de esos datos. Recuerda que las fotos de actividades con los alumnos debes entregarla lo más pronto posible al responsable (Jefa de Estudios), y después destruirlas.

4. MÓVILES

El tamaño pequeño del teléfono favorece su portabilidad (hay gente que incluso lleva dos, el personal y el profesional), y eso es indudablemente una gran ventaja, ya que es posible llevarlo a todos sitios (al trabajo, al cine, de viaje, incluso al baño) sin ningún esfuerzo. Pero al mismo tiempo supone un claro inconveniente: la posibilidad muy real de dejarlo olvidado en algún sitio (el 98 % de las tablets y ordenadores portátiles perdidos nunca se recuperan), que nos lo roben o que alguien con malas intenciones intente acceder a nuestros datos personales o profesionales.

4.1 Medidas de control de los datos compartidos

- Para evitar dejar una puerta abierta a que nos envíen archivos o enlaces no deseados trata de dejar desactivado el Bluetooth cuando no los estés usando.
- Desconecta la opción Wi-Fi del teléfono cuando no estés en casa ni en el

trabajo, no te conectes nunca a una red pública, y evita en la medida de lo posible las redes privadas que te faciliten la contraseña, como es el caso de cafeterías, hoteles, hospitales, etc.

4.1. Medidas de control remoto del dispositivo en caso de pérdida o robo

SISTEMA OPERATIVO iOS (APPLE)

Apple tiene todos los datos de tu iPhone cifrados, así que es prácticamente imposible que te roben los datos, aunque tengan tu teléfono físicamente, mucho más si tienes el sistema de reconocimiento de huella o facial. Aquí tienes el link que te lleva a la ayuda de Apple sobre cómo actuar en caso de pérdida o robo:
https://support.apple.com/es-es/HT201472

SISTEMA OPERATIVO ANDROID

Android no tiene tus datos cifrados, y no es excesivamente difícil acceder a tus datos a alguien que sepa hacerlo, y tenga tu teléfono físicamente. Así que atento ahora.

Las medidas de control serán las siguientes y en el orden que vienen:
Antes de la pérdida o robo:

- Tener activada la opción de localizar, bloquear y borrar el dispositivo de Android desde el administrador de dispositivos.
- Apuntar el IMEI del dispositivo, junto con el número de serie.

Después de la pérdida o robo:

- Si tenemos dudas de si lo hemos perdido en algún lugar próximo, activar reproducir sonido, para que el teléfono suene durante 5 segundos a todo volumen.
- Si se trata de un robo, localizar, bloquear o borrar toda la información a través de Android. Escribir en google: android.com/find. Se entra a través de la cuenta de Google.
- Posteriormente se llamará a la operadora para bloquear el acceso a la red del móvil y de nuestra SIM, y se pondrá la denuncia en la policía.

Samsung, herramienta “Find my mobile”: https://www.samsung.com/es/a-fondo/contenidos-y-servicios/find-my-mobile-localiza-tu-movil-extraviado/

Sobre las actualizaciones del sistema o apps

Comprobar regularmente que el sistema está en la última versión para que esté parcheado en la opción “Actualizar sistema del teléfono”.
De igual forma, las aplicaciones deberán estar actualizadas en su última versión.

Copia de seguridad: cómo y cuándo se hará

Esto es importante porque perder los archivos significa perder recuerdos, contactos, trabajo, etc. Para evitarlo puedes realizar lo siguiente:

SISTEMA OPERATIVO iOS (APPLE)

- Realizar un Backup (el teléfono o i-Pad te avisa cada semana)

- Tener espacio suficiente en i-Cloud, y tus datos se van guardando ahí, encriptados. Ni si quiera Apple accede a ellos.

SISTEMA OPERATIVO ANDROID

- Tener activado en el teléfono la Copia de seguridad de datos vinculada a la cuenta de Copia de seguridad, así como la restauración automática.
- Realizar una copia de seguridad de los contactos, mensajes, aplicaciones y del contenido multimedia en el ordenador. Con Huawei esto se realiza a través de www.huawei.com/hisuite
- Se recomienda realizar una copia de seguridad cada mes.

De la misma forma puedes sincronizar el dispositivo móvil con Google Drive (datos no encriptados), que guarda el contenido multimedia de forma automática en la nube.

5. REDES

La EOI dispone de dos redes, una administrativa y otra docente. A ésta última es posible conectarse de forma inalámbrica, mediante wifi, y es exclusiva para uso de los profesores en su labor didáctica. Por motivos de seguridad está prohibido ceder la contraseña a ninguna persona que no sea docente de la EOI. Esta contraseña se cambiará de forma regular, al menos una vez al año, y será facilitada a los profesores.

RESUMEN RÁPIDO

Cosas “to do”

- Escaneado completo del ordenador (antivirus y antimalware) cada mes.
- Actualiza el software siempre, y cuanto antes.

Copias de seguridad cada mes, en disco duro cifrado del departamento.