SEGURIDAD EN EL AULA

J. CARLOS FERNÁNDEZ RODRÍGUEZ
ALICIA RAMOS ALCALDE

> Si tu empresa gasta más en café que en seguridad TI, serás hackeado. Es más merecerás ser hackeado.

—Eric S. Raymond

> Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes la tecnología. El usuario escogerá cerdos bailando antes que seguridad, una vez tras otra.

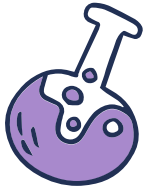
—*Bruce Schneiner*

> “Las empresas invierten millones en firewalls, cifrado y dispositivos para acceder de forma segura y es dinero malgastado, porque ninguna de estas medidas corrige el nexo más débil de la cadena, el usuario.”
>
> —Kevin Mitnick

Dos focos

Usuarios

Medidas que se deben tomar en los dispositivos de los usuarios e información.



Organización

Medidas que tomará la organización sobre sus equipos, dispositivo de red e información.

Organización

1

Equipos del personal

¿Qué pueden y no hacer?

2

Copias de seguridad

¿Tenemos y sabemos guardar nuestros datos?

3

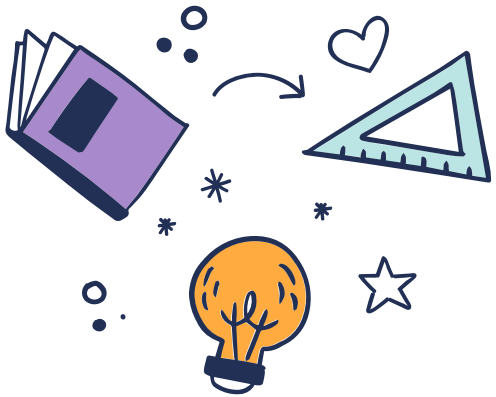
Cifrado

¿Protegemos correctamente nuestros datos?

DISPOSITIVOS DEL PERSONAL

Punto clave

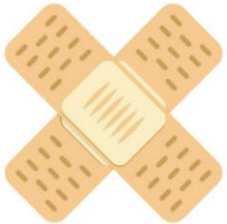
Dispositivos



A día de hoy en el aula y en el centro educativo convergen multitud de dispositivos y SO, desde tabletas a portátiles pasando por teléfonos. Que pueden tener Linux, Android, Windows, iOS.....

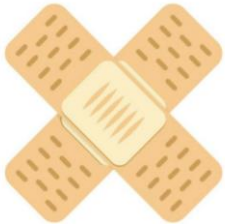
- Muchos se conectan a nuestra red del cole. Y otros directamente son del cole por lo que están conectados por defecto.
- ¿Qué condiciones ponemos? Si delinquen desde la red del cole hay un registro.....

Seguridad de usuarios



En el cole obligamos a ir, vestidos, ahora usamos mascarilla...
Para circular con un coche nos obligan a que tenga frenos, cinturón de seguridad...
¿Por qué dejamos que los dispositivos se usen de cualquier manera?
Antivirus, proxy... por lo menos,
CUIDEMOS LOS DISPOSITIVOS DE NUESTRO CENTRO

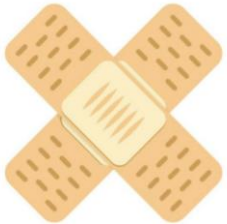
Seguridad de usuarios



Cosas que podemos hacer en nuestros equipos:

- Antivirus.
- Navegación privada.
- ¿Registros de usuarios?
- Contraseñas

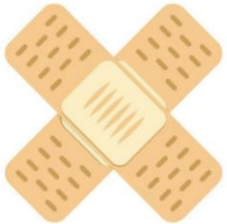
Antivirus



Partimos de la base que no soy comercial de Antivirus.

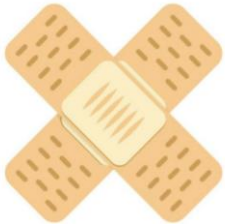
- El **antivirus** no es la cura de todos los males; de hecho, si lo elegimos mal puede ser el peor de los males.
- GRATUITO, Windows tiene el suyo, pero no suele salir muy bien parado. Aún así, es la solución más ágil y cómoda.
- En los ordenadores del centro debería ser obligatorio.
- ¿Y en el de los alumnos?

Antivirus



Clasificación totalmente independiente y web bastante interesante, AQUI

Navegación privada



Es la opción más segura para los ordenadores comunes.

No deja registro de nada, QUE SUENA LA CAMPANA PARA EL CAMBIO DE CLASE... al cerrar el navegador se cierran todas las sesiones: gmail, educajcyl ...

Os explico como poner el navegador por defecto en navegación privada.

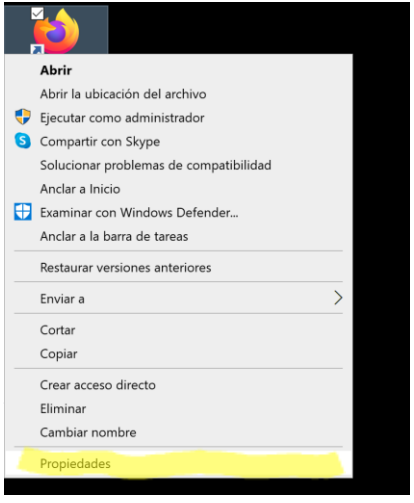
Navegación privada

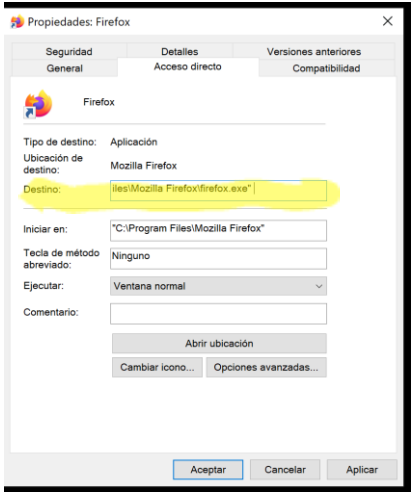
Un gesto bastante fácil

1. Tanto en Firefox, EDGE, IE y Google Chrome hace de la misma manera:
Pinchamos con el botón secundario del ratón sobre el icono del acceso directo del navegador y después en propiedades.

2. Pinchamos en acceso directo y después en Destino.

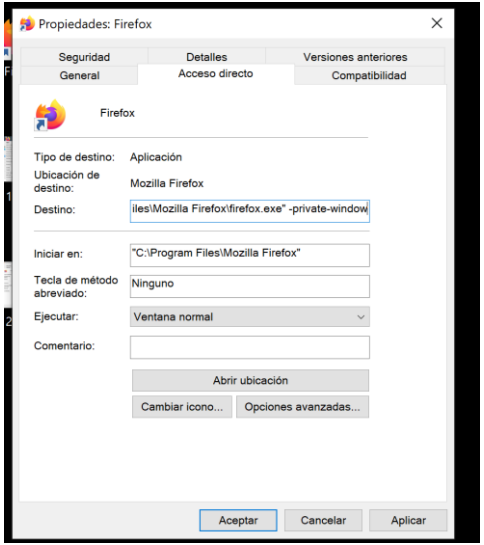
3. Nos iremos al final de la linea tras las comillas y en cada navegador tenemos que introducir algo diferente.

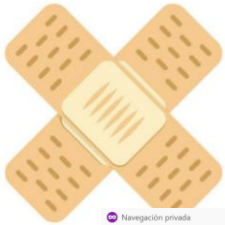


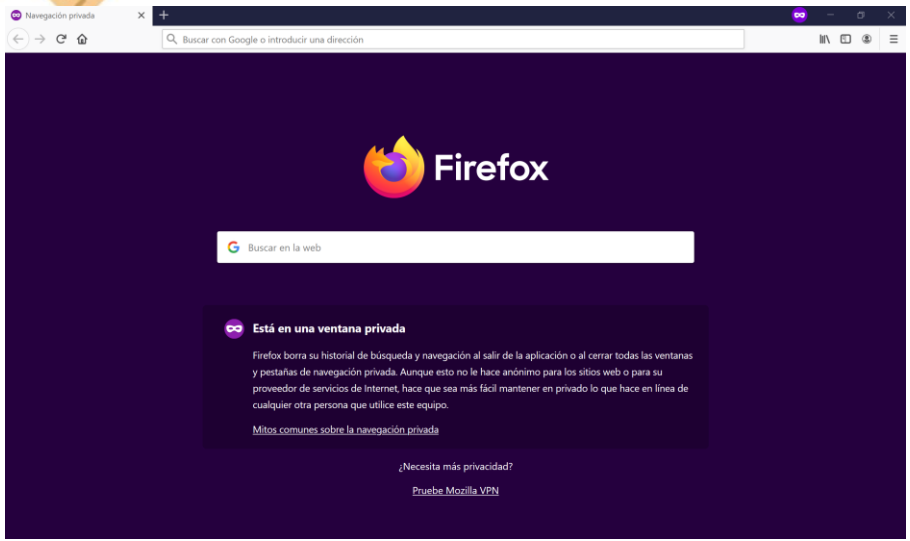


- **Firefox:** Añadiremos tras la" un espacio y ´prívate-window´ (sin las comillas).
- **EDGE e IE:** Añadimos tras la" un espacio y '–private' (sin comillas).
- **Chrome:** Añadimos tras la" un espacio y '–incógnito" (sin comillas)

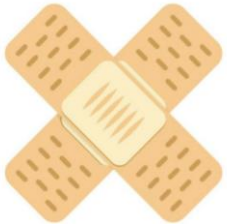
Navegación privada





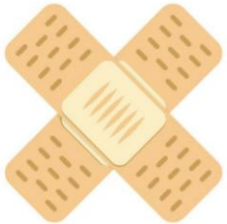


Registro de usuarios



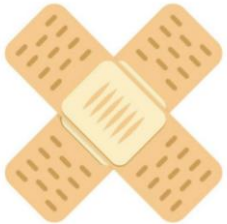
- ¿Qué pasa si se comete un delito desde el colegio?
-¿Quién/es serían los culpables?
- ¿Responsable civil subsidiario?

Registro de usuarios



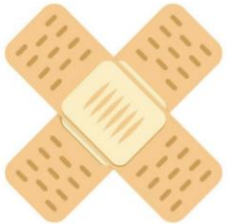
- Control de MAC y de quién usa los dispositivos del colegio.
- Control de redes WIFI

Contraseñas



Probablemente en el cole se usen pocas contraseñas, pero...
¿Quién y cómo las guarda?
¿Y si está de baja laboral o se muere?

Contraseñas



Programas gestores de contraseñas. Una contraseña maestra abre todas las contraseñas. Se almacena con seguridad la base de datos. Sin la contraseña maestra no se pueden sacar las mismas. Es un proceso que no lleva más de 1 minuto y nos ayudará ante contingencias.

KeePass

Copias de Seguridad

Ese gran olvidado...

Copias de Seguridad

De manera académica es un proceso mediante el cual duplicamos la información existente **de un soporte a otro,** con el fin de poder recuperarlos en caso de fallo del primer alojamiento

Copias de Seguridad

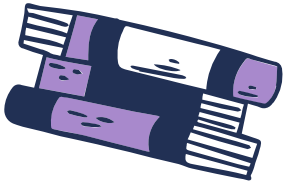
Para mí es la salvaguarda de nuestro negocio, trabajo o vida, es la medida indispensable para garantizar que ante cualquier contingencia podemos continuar trabajando sin grandes traumas.

Copias de Seguridad

En vuestro caso la JCyL, hace copias del programa colegios…. Pero ¿El resto de datos también?… ¿o los dejamos en nuestro ordenador?

¿Un robo, un fallo del disco duro…..?.

INFORMACIÓN



En los modelos teóricos hay varias clasificaciones de la información, dos de las que se os pueden aplicar son:

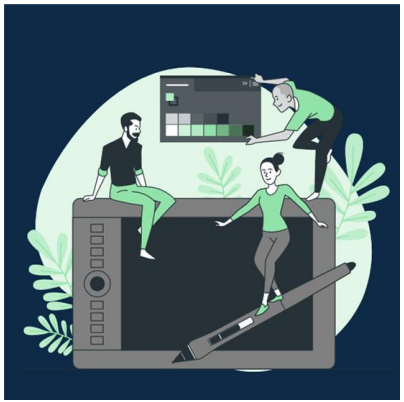
- **Por nivel accesibilidad o confidencialidad.**
  - **Confidencial:** Accesible solo a personal concreto o a la dirección.
  - **Interna:** Aquella que es solo para personal interno o grupos de personal de la organización.
  - **Pública:** Accesible públicamente.
- **Por el impacto en caso de pérdida de información:**
  - **Daño a la imagen**
  - **Consecuencias legales**
  - **Consecuencias económicas**
  - **Paralización de la actividad**

INFORMACIÓN

CATEGORÍA	DEFINICIÓN	TRATAMIENTO
Confidencial	Información especialmente sensible para la organización. Su acceso está restringido únicamente a la Dirección y a aquellos empleados que necesiten conocerla para desempeñar sus funciones. También datos de carácter personal, en particular los de categorías especiales.	Esta información debe marcarse adecuadamente. Se deben implementar todos los controles necesarios para limitar el acceso únicamente a aquellos empleados que necesiten conocer la información. En caso de sacarla de las instalaciones de la empresa en formato digital, debe cifrarse. Para los datos de carácter personal, se deben tener en cuenta la protección y garantías indicadas en la legislación sobre la materia.
Interna	Información propia de la empresa, accesible para todos sus empleados. Por ejemplo, la política de seguridad de la compañía, el directorio de personal u otra información accesible en la intranet corporativa.	Esta información debe estar adecuadamente etiquetada y accesible para todo el personal. No debe difundirse a terceros, salvo autorización expresa de la dirección de la empresa.
Pública	Cualquier material de la empresa sin restricciones de difusión. Por ejemplo, información publicada en la página web o materiales comerciales.	Esta información no está sujeta a ningún tipo de tratamiento especial.

Tabla de INCIBE

PERIOCIDAD Y TIPO DE COPIAS



- **Número de datos o archivos generados/modificados**
- **Coste económico y de espacio de almacenamiento.**
- **Obligaciones legales, RGPD**

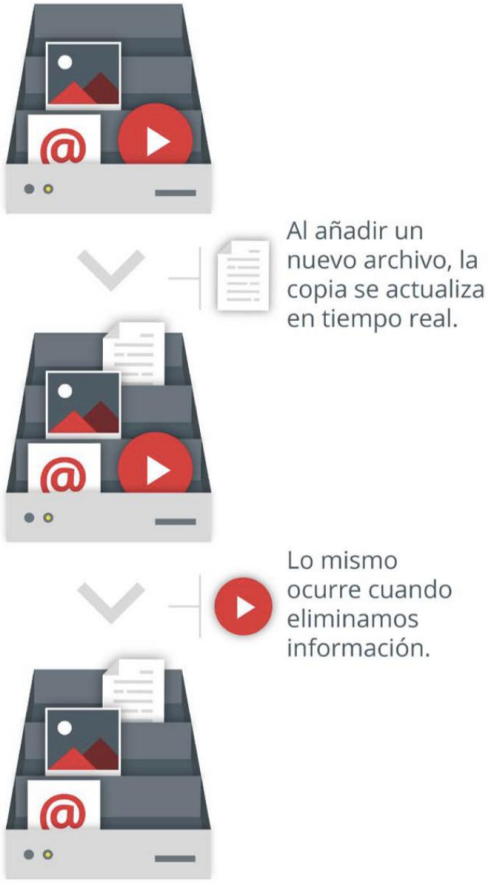
Tipos de copias de seguridad.

HAY MÁS

Espejo o RAID 1

En tiempo real se hace la copia de seguridad, no se almacenan archivos antiguos o en desuso, la recuperación es muy rápida ya que es entrar a la copia y descargar el archivo que queramos.
Inconveniente: si lo borramos del equipo lo borras de la copia.

Hay un híbrido como Time Machine.



Tipos de copias de seguridad.

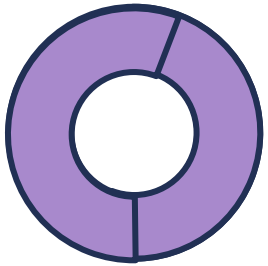
HAY MÁS

Imagen

Personalmente la más importante, y muy poca gente conoce o hace. Consiste en una copia exacta de nuestro ordenador en un punto concreto del tiempo. Cuando la restauramos el ordenador vuelve a ese punto, como nuevo. NADA QUE VER CON UN PUNTO DE RESTAURACIÓN. Momento idóneo tras montar el ordenador.

Tipos de copias de seguridad.

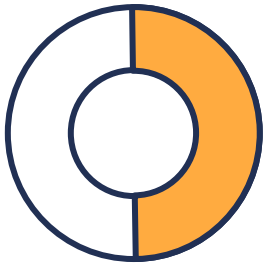
HAY MAS



100%

Completa

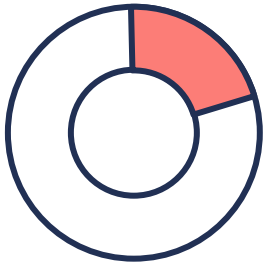
Copia todos los archivos que le digamos sin distinción



% De Completa

Diferencial

Solo copia lo cambiado de la anterior completa.



% de cualquier

Otra copia

Realiza la copia de los archivos modificados desde la última copia.

Explicación rápida

Vaya lío no????

Nosotros

Nos tendremos que preguntar qué datos tenemos o queremos conservar. No es una pregunta baladí, es una pregunta de profunda reflexión, si no lo tomamos así, el día que perdamos los daos nos daremos cuenta de aquello que necesitábamos,

Tiempo

Tenemos que buscar una solución que se adapte a nuestro tiempo y cantidad de archivos. Automatización.

Nuestros archivos

Tipos de archivos ¿se almacenan ya solos en la nube? ¿es eso seguro? ¿cumple ese almacenamiento con nuestras necesidades? ¿Es seguro ese almacenamiento?

Planificación, documentación, ejecución y... probar

Antes de empezar como locos, tendemos que planificar cómo y porqué, DOCUMENTAR, el que venga detrás lo agradecerá y, sobre todo, probar si funciona dicha copia

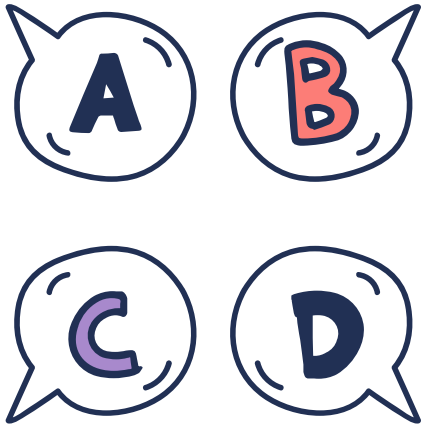
Como empiezo

La aplicación

Multiplataforma, segura, GRATIS, si puede ser Software Libre mejor.

Almacenamiento

Lugar donde se almacenarán, lo más lejos posible de la información original



La planificación

Tipos de copias, días, horas....

Encargado

Persona o personas encargadas de la custodia y realización de las mismas.

Aplicaciones

- Hay diversas aplicaciones. Deben cumplir algunas características para que nuestras copias sean lo mas “universales” posibles:

- ❑ Multiplataforma.
- ❑ Gratis, SOFTWARE LIBRE A PODER SER.
- ❑ Testado.
- ❑ Múltiples formatos y lugares de copias.
- ❑ “Facilidad de uso”

Aplicaciones

- **Cobian Backup;** tiene más años casi que los ordenadores, pero personalmente es, si no la mejor, de las mejores en su sector, es la típica aplicación que a día de hoy por la interfaz se ve “vieja”, pero su funcionamiento es impecable, además, es muy intuitiva. Quizás debería permitir el subir las copias a servidores online, no solo por FTP.

- **Parangon Backup & Recovery;** Es más visual y para usuarios “Siguiente, siguiente”, pero es software propietario.

- **Macrium reflect;** Tiene Versión gratuita, es otro “siguiente siguiente” pero mucho más completo, permite imágenes, guardar solo archivos de correo… mucha personalización.

- **Duplicati;** Es una versión mejorada y más moderna de Cobian, de hecho, tienen parte del equipo de programadores que se fue de Cobian, permite subir las copias a OneDrive, Dropbox…

¿Dónde las almaceno?

Mil opciones en el mercado, desde miles de euros hasta gratis pasando por 10-20€.

- **Nubes de empresas,** hay empresas que se dedican a las copias de seguridad con su programa exclusivo, es una opción bastante cara, pero en la que descargamos la responsabilidad.

- **Nubes "públicas",** muchos programas permiten subir directamente las copias a: OneDrive, Dropbox, Mega... que tienen planes gratuitos de alojamiento o bastante económicos. Aunque las copias las guarde esa empresa, no es una empresa de copias de seguridad al uso, por lo que tendremos que leer los TC, para comprobar qué pasa si se pierde un documento o cumple la RGPD.

- **Dispositivos físicos**, tenemos varias opciones desde pincho USB, a NAS, pasando por las cintas de toda la vida o un disco duro externo.

Identificación

Tipo de copia y nombre

Para saber qué restaurar, no pongamos COPIA 1, COPIA 2...

Fecha hora y almacenamiento

Hay que tener detallada la fecha, así como dónde está

Personal

Importante saber quién la ha hecho.

Como lo podríamos hacer

	Completa	Diferencial	Incremental
Poca modificación de archivos	Último día del mes	Una quincenal	Una a la semana
Trabajo casi diario de modificación archivos	Días 15 y último de mes	Una a la semana	Una cada dos días
Trabajo continuo de modificación de archivos	Una semanal, último día de la semana	Cada 48h	Una diaria

¿Cuánto tiempo las mantengo?

Completas

1 curso, un trimestre....

Diferencial

Junto con las completas mas o menos el mismo tiempo

Incrementales

Un mes

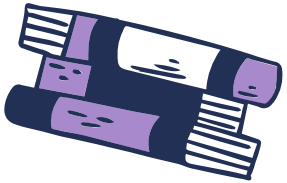
NO CUMULAR

No guardemos 500 copias de 300 años.

Cifrado

No nos metamos en la cripta

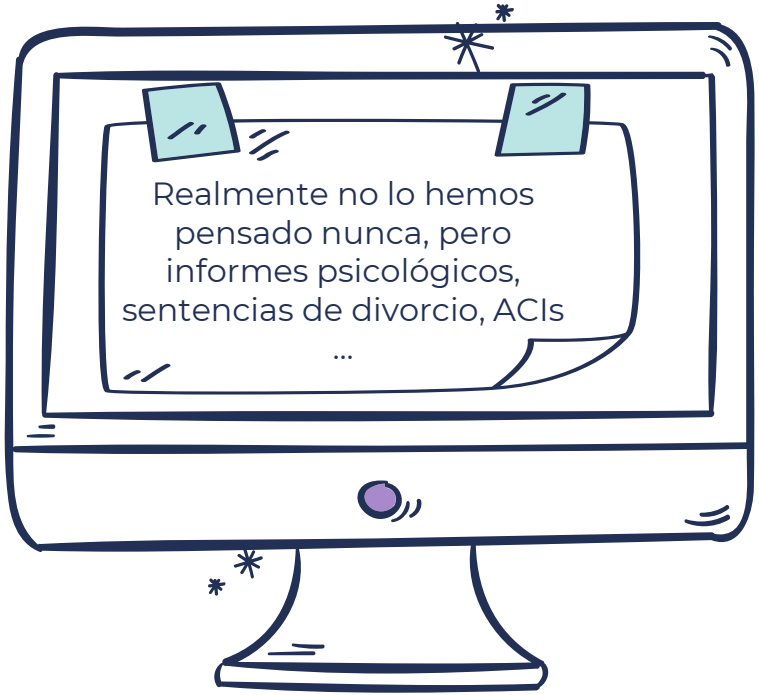
INFORMACIÓN



En los modelos teóricos hay varias clasificaciones de la información, dos de las que se os pueden aplicar son:

- **Por nivel accesibilidad o confidencialidad.**
  - **Confidencial:** Accesible solo a personal concreto o a la dirección.
  - **Interna:** Aquella que es solo para personal interno o grupos de personal de la organización.
  - **Pública:** Accesible públicamente.
- **Por el impacto en caso de pérdida de información:**
  - **Daño a la imagen**
  - **Consecuencias legales**
  - **Consecuencias económicas:**
  - **Paralización de la actividad**

Para qué voy a cifrar si yo solo uso...



Cientos de documentos sensibles

Muchas veces sin control alguno.

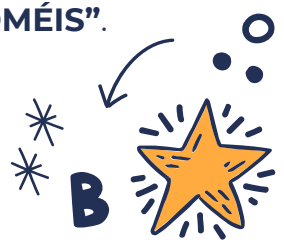
La Junta, el director, el encargado, la ... y así un largo etc...

Descargamos responsabilidad

¿Quién recibiría la sanción?

En nuestra legislación existe la figura de “responsable civil subsidiario”, es decir, aunque “la cague” estoy protegido por el manto de mi empresa (Estado, JCyL...).
En tema de protección de datos, tras consultar con varios abogados, “el estado no puede ser nunca sancionado”.

ES DECIR: “OS LA COMÉIS”.



Aplicaciones

Cuenta EDUCA

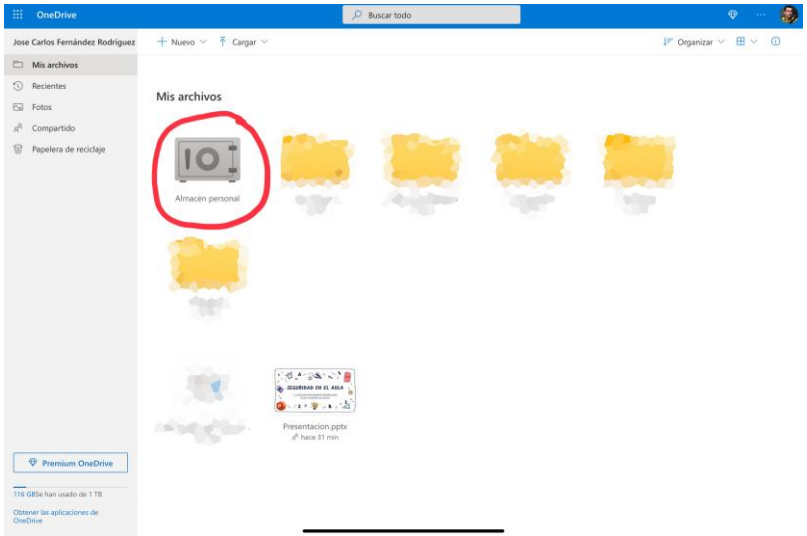
- En teoría vuestra cuenta EDUCA, está “comprometida” con la seguridad y la RGPD.
- Todo aquello que subamos a nuestro ONEDRIVE, cumple con la RGPD, con todos los criterios de seguridad…
- Pero somos los responsables del uso de dicha cuenta, es decir: ¿cuántas veces nos hemos dejado la cuenta abierta? recuerdo en una ponencia… Dejamos nuestro ordenador a alguien con la cuenta metida, tengo acceso a todos los ficheros… Un robo…
- Todo mal uso que demos y comprometa nuestros datos “nos la comememos nosotros”.
- TENDRÍAMOS QUE USAR EL **ALMACÉN PERSONAL**

Aplicaciones externas

- Hay aplicaciones que antes de subir estos datos los cifran con protocolos bastante seguros por lo que ante un robo, mal uso, no podrán ver esos datos sensibles.
- No hay que ser paranoico, pero hay archivos sensibles y es mejor perder 3 minutos cifrando y descifrando que perderlos.
- Es compatible el subir el archivo a educa, pero cifrado, es decir protegido.
- VeraCrypt.

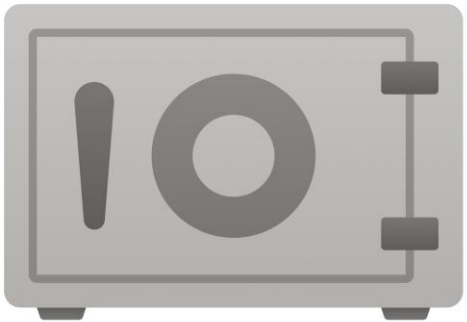
Almacén personal

Dentro de OneDrive, estoy YO, soy el Almacén personal.



Almacenamiento personal

- Es un apartado reservado dentro de OneDrive.
- Nos obliga a una segunda autenticación, ya sea vía “volver a iniciar sesión” o “mandando un sms o código” a una cuenta secundaria que tengamos registrada.
- Es una solución rápida y fiable (al menos eso dice Microsoft).



Almacén personal

Gracias

Podéis encontrarme como
@cafero91 por el ciberespacio