Universidad Zaragoza

1542

Servicio de **Informática y Comunicaciones**

Charla de concienciación frente a Malware

Medidas y buenas prácticas

Malware

Ransomware

¿Qué es el malware?

*"Todo software o actos creados para afectar maliciosamente a los sistemas informáticos es **malware**"*

*"**Ransomware** es malware que cifra los datos del usuario, solicitando un rescate económico e infectando a otros equipos"*

*"**Phising** es malware que mediante técnicas de ingeniería social hacen que un usuario introduzca sus credenciales en una web que no es en realidad la que parece"*

- **Está siendo un negocio muy lucrativo. No es un hacker solitario … son auténticas mafias**

- **No es una moda pasajera -> ha venido para quedarse**

- **Cada vez va a más -> más dispositivos -> IoT**

Equipo infectado

Equipo infectado

Cómo actuar en caso de infección

Hay que ser rápido y de inmediato, para evitar contagios:

1. **Guardar documentos y APAGAR EL EQUIPO**
2. Notificar de inmediato al SICUZ

1. Si aparece en mi pantalla el **mensaje de equipo infectado**
2. O bien, **no podemos abrir varios documentos**
3. O bien … nos hemos dado cuenta de **haber "clickado" en un link** de correo fraudulento sin querer
4. O, se han **puesto en marcha sin intervención** equipos que estaban apagados

Apagar el equipo y
avisar a vuestro Técnico del **SICUZ** cuanto antes

Situación actual

Situación actual … y hablamos de ahora!

ComputerHoy.com

Servicios públicos de todo el país están caídos por un ataque ransomware a su proveedor en la nube ASAC

Servicios públicos de todo el país están caídos por un ataque ransomware a su proveedor en la nube ASAC. Noticia. ASAC servicios en la nube.

Hace 1 día

La Vanguardia

La mayor red de oleoductos de EE.UU. paralizada por un ataque de "ransomware"

Colonial, la mayor red de oleoductos de Estados Unidos, ha tenido que paralizar todas sus operaciones por un ataque de "ransomware" en el ...

Hace 1 día

IT Reseller

El ransomware es cada vez más profesional y los ataques ...

Los ciberdelincuentes están constantemente innovando, a la caza de vulnerabilidades para lanzar oleadas de ransomware. Además del robo ...

Hace 20 horas

elDiario.es

Hazte socio/a Inicia sesión

Castilla-La Mancha

Coronavirus en Castilla-La Mancha ¿Quiénes somos? Agroalimentaria Viajes Nuestros blogs Apúntate al bolet...

El programa malicioso Ryuk, causante del ciberataque en la Universidad de Castilla-La Mancha, el mismo que hizo caer al SEPE

La Institución académica confía en recuperar los datos y los servicios digitales de la UCLM "en próximos días" tras el ataque "premeditado contra la infraestructura crítica de la universidad"

Efectos de **Ryuk** -> el del SEPE o la UCLM

Es un ransomware que básicamente lo que nos hace es:

1. **Cifra los documentos locales** o en **unidades de red de carpetas compartidas** mediante una clave criptográfica y **pide rescate económico** (criptomonedas) para poder descifrarlos. **El pago no garantiza la recuperación**
2. **Intenta arrancar** equipos apagados (para posteriormente intentar infectarlos)
3. **Sondea la red y subredes adyacentes** para afectar a otros equipos y así seguir replicándose
4. Es **transparente al usuario**. No se percata (salvo en equipos antiguos debido a su lentitud al encriptar documentos grandes)
5. Cuando aparece el **pantallazo**, ya ha cifrado tu equipo

Informe de CCN-CERT Código Dañino Ryuk

¿Cómo se contagia?

Agujeros de seguridad en sistemas, servicios y programas

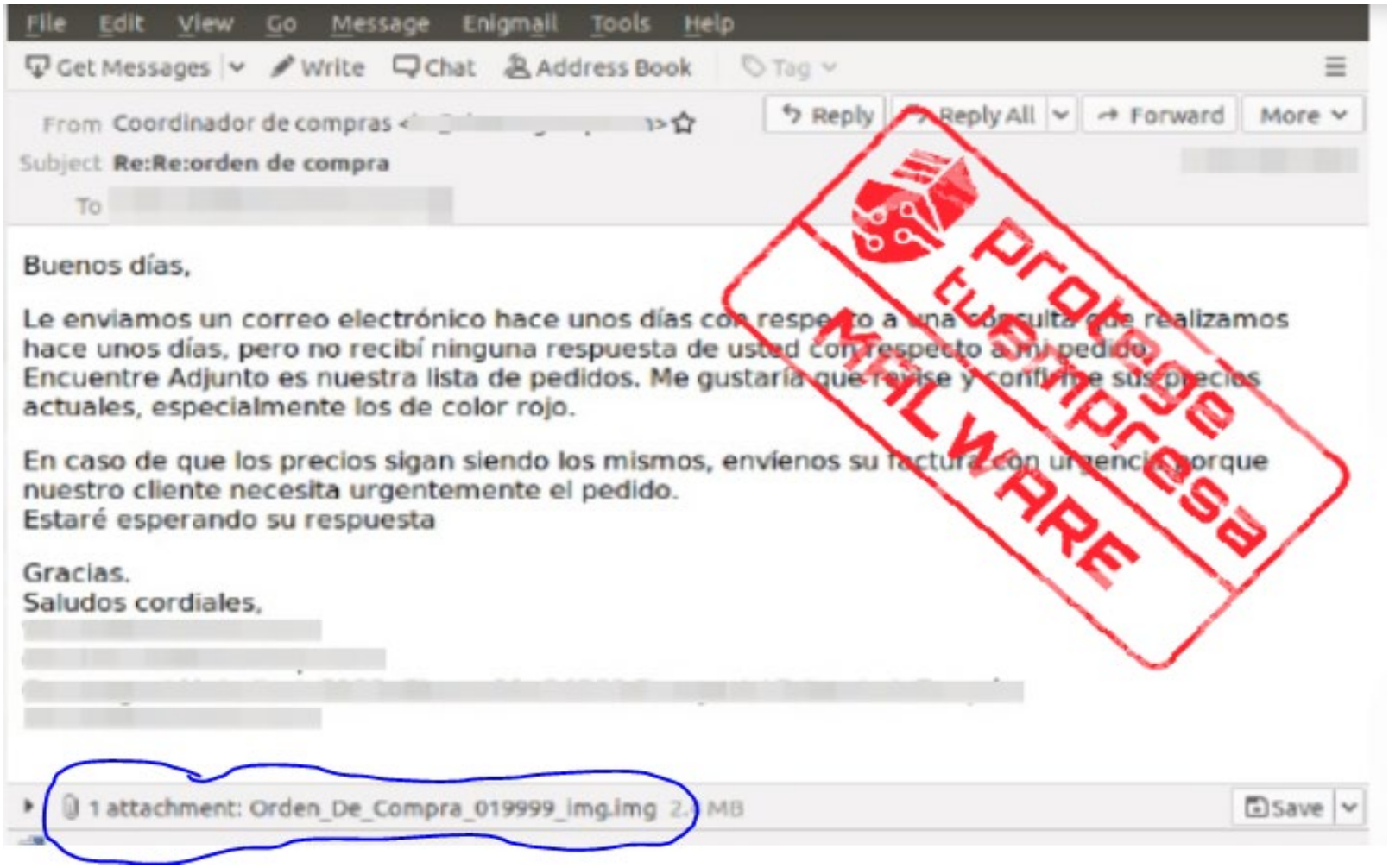
Equipos desactualizados

Descuidos y errores humanos

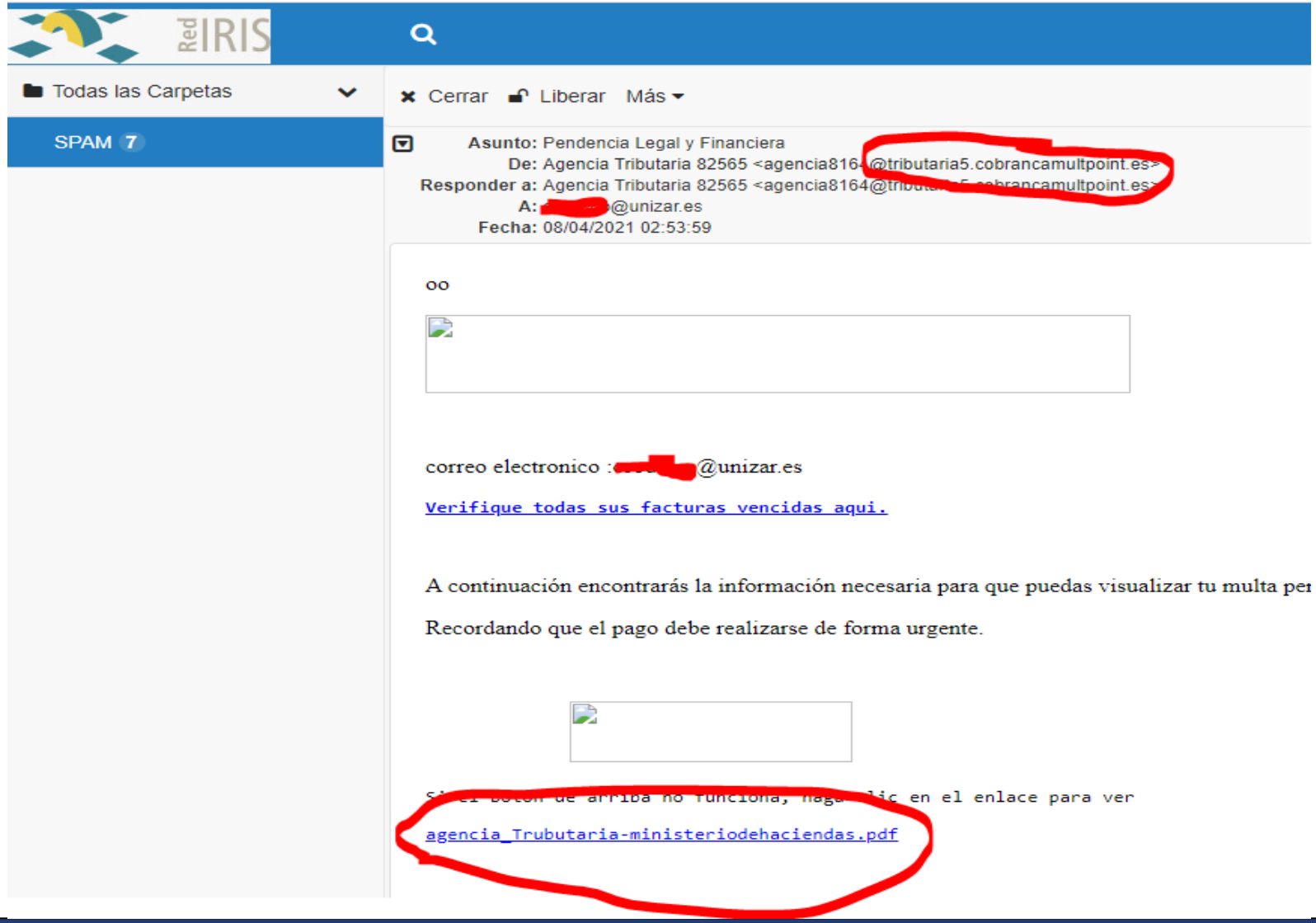
Principales vectores de entrada

- **correo malicioso** -> adjunto ejecutable -> link
- **penDrive** infectado
- **macros** de Office de dudosa procedencia.

Ejemplo de correo malicioso “detectable”

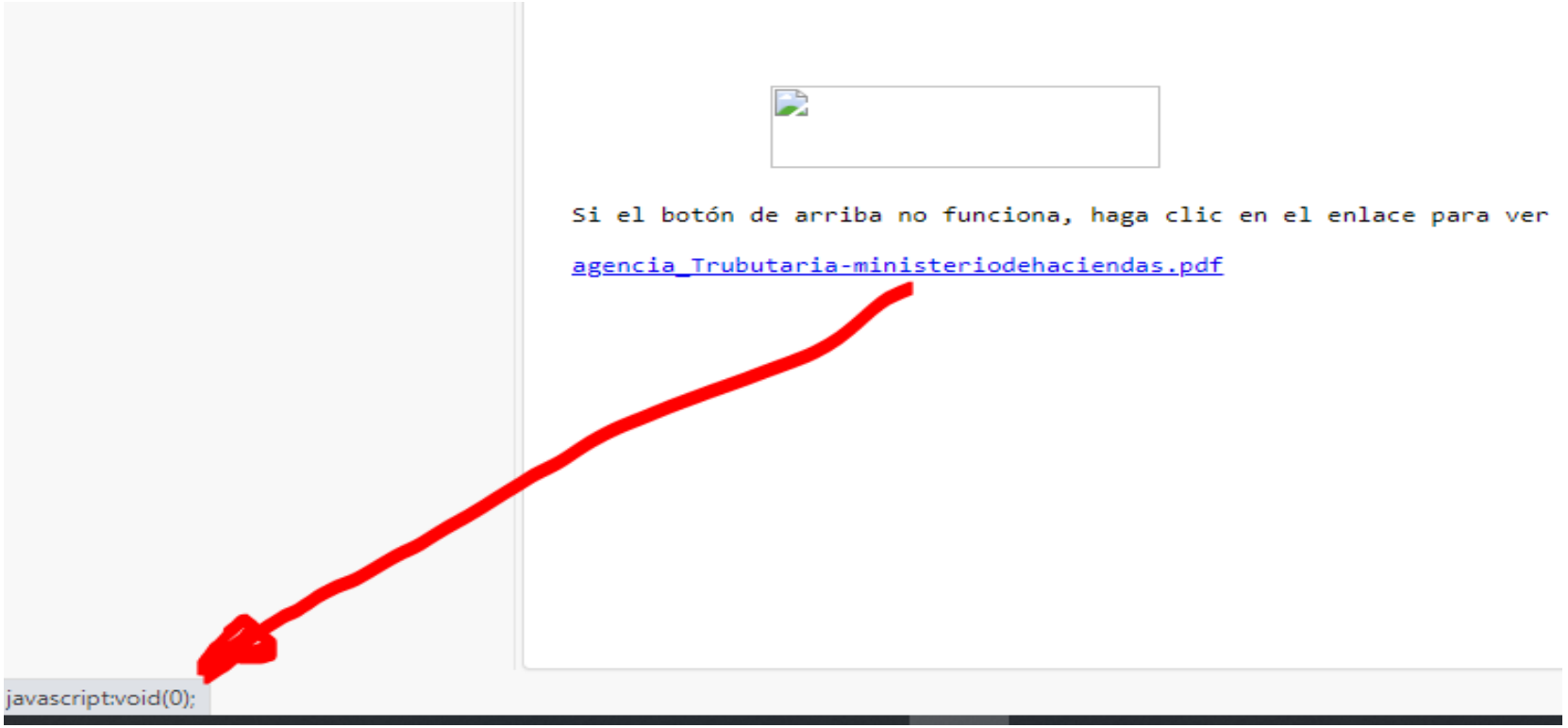


Ejemplo de correo malicioso “detectable a la vista”



Ejemplo de correo malicioso “detectable a la vista”
enlace a código Javascript”

El texto del enlace no tiene por qué coincidir con el enlace real



Ejemplo de correo malicioso “confiable a la vista”

CORREOS

Su paquete ha llegado **15 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

Descargar información sobre su envío

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de **8,27** euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Privacidad

Se pone en conocimiento de los usuarios cuyos datos de carácter personal estén incorporados en ficheros de Correos, que podrán ejercitar los derechos de acceso, rectificación, cancelación y oposición de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. A estos efectos, podrá optar por contactar con Correos a través del teléfono 902 197 197 o dirigir escrito acompañándolo de copia del Documento Nacional de Identidad o documento equivalente, a la Sociedad Estatal Correos y Telégrafos S.A. C/ Vía Dublín nº 7 - 28070 Madrid; lo anterior sin perjuicio de las utilidades de acceso, rectificación y revocación del consentimiento que, en su caso, Correos hubiera puesto a disposición del usuario en las pantallas de los respectivos servicios. Correos garantiza que ha adoptado las medidas oportunas de seguridad en sus instalaciones, sistemas y ficheros, así como la confidencialidad de sus datos de carácter personal..

Haga clic aquí para darse de baja.

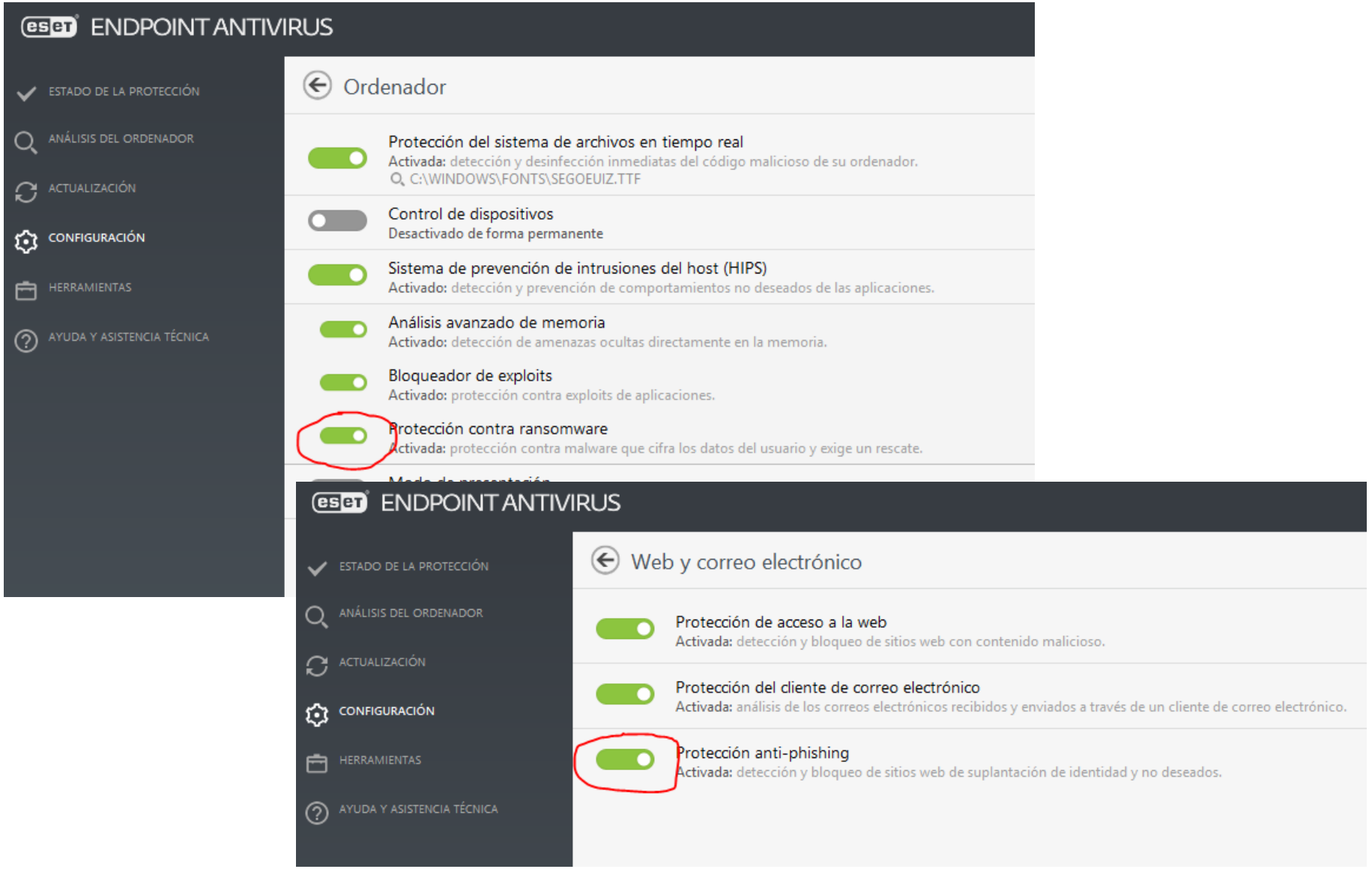
Acciones Preventivas por parte del SICUZ

Acciones preventivas tomadas por parte de SICUZ

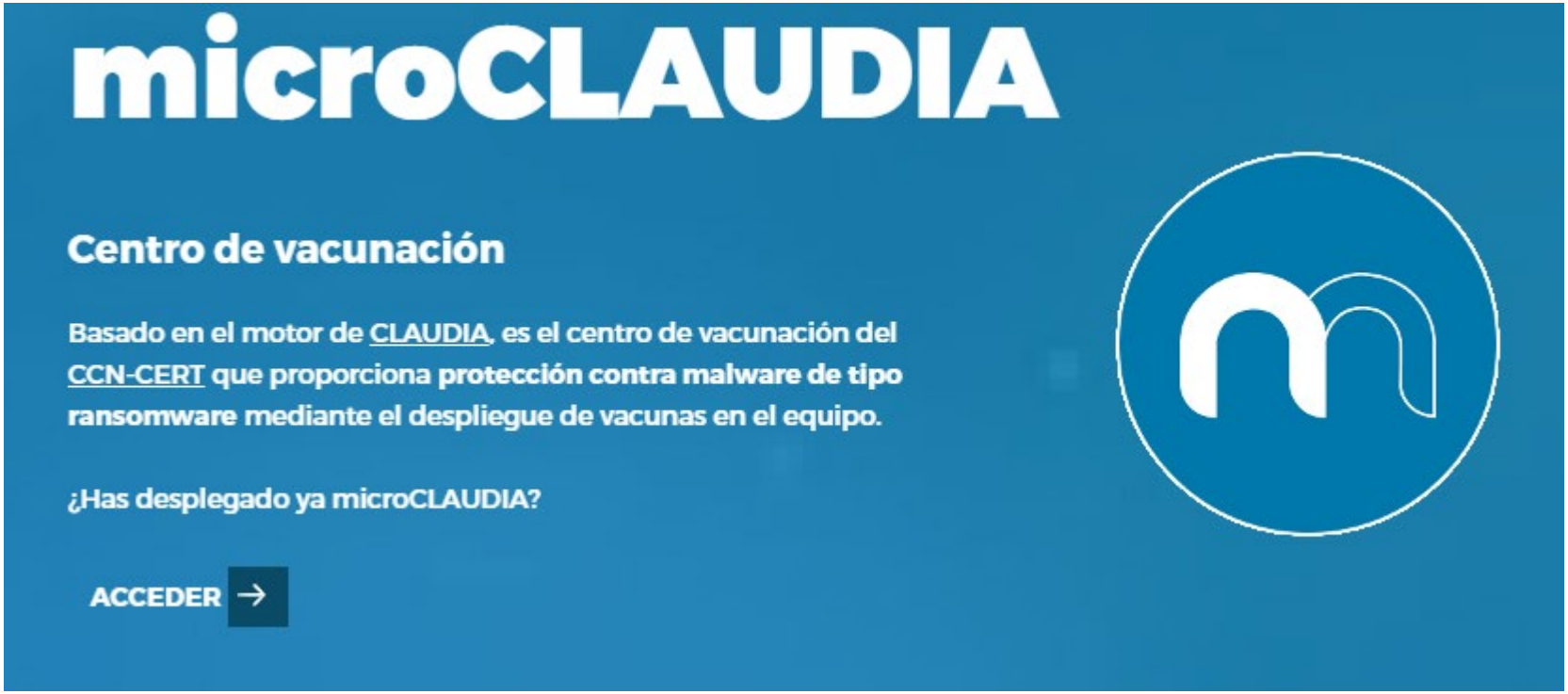
- A nivel de servidores -> **SICUZ** Área Sistemas (Refuerzo Copias, Actualización Sistemas, etc ...)

- A nivel de red -> **SICUZ** Área Comunicaciones (Monitorización y Alertas, etc ...)

- A nivel de ordenadores personales -> **SICUZ** Área Usuarios recomienda:
  - Migrar equipos win XP, 7 -> win10 (equipos que puedan soportarlo)
  - Actualizaciones automáticas win10 activadas
  - Antivirus ESET última versión (8) disponible en Unizar (licencia disponible sólo equipos propiedad de la universidad).
  - **SALVAGUARDAR DATOS LOCALES PREFERENTEMENTE EN UNIDAD DE DISCO EXTERNA USB EN GOOGLE DRIVE O MICROSOFT ONEDRIVE**


ENDPOINT ANTIVIRUS
ESTADO DE LA PROTECCIÓN
ANÁLISIS DEL ORDENADOR
ACTUALIZACIÓN
CONFIGURACIÓN
HERRAMIENTAS
AYUDA Y ASISTENCIA TÉCNICA
Ordenador
Protección del sistema de archivos en tiempo real
Activada: detección y desinfección inmediatas del código malicioso de su ordenador.
C:\WINDOWS\FONTS\SEGOEUIZ.TTF
Control de dispositivos
Desactivado de forma permanente
Sistema de prevención de intrusiones del host (HIPS)
Activado: detección y prevención de comportamientos no deseados de las aplicaciones.
Análisis avanzado de memoria
Activado: detección de amenazas ocultas directamente en la memoria.
Bloqueador de exploits
Activado: protección contra exploits de aplicaciones.
Protección contra ransomware
Activada: protección contra malware que cifra los datos del usuario y exige un rescate.
ENDPOINT ANTIVIRUS
ESTADO DE LA PROTECCIÓN
ANÁLISIS DEL ORDENADOR
ACTUALIZACIÓN
CONFIGURACIÓN
HERRAMIENTAS
AYUDA Y ASISTENCIA TÉCNICA
Web y correo electrónico
Protección de acceso a la web
Activada: detección y bloqueo de sitios web con contenido malicioso.
Protección del cliente de correo electrónico
Activada: análisis de los correos electrónicos recibidos y enviados a través de un cliente de correo electrónico.
Protección anti-phishing
Activada: detección y bloqueo de sitios web de suplantación de identidad y no deseados.

Acciones preventivas tomadas por parte de SICUZ



Copias de seguridad

En caso de una infección **el SICUZ podrá restaurar copias de sus servidores carpetas compartidas, de moodle, de documenta, de lo que tenga en sus servidores**, etc

Se podrán restaurar los equipos de trabajo a como estaban recién instalados, con sus programas **pero no con sus datos**

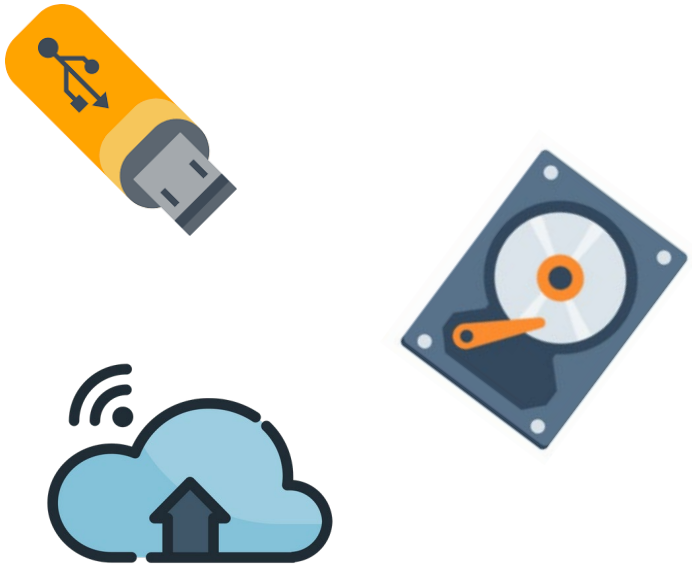
Los datos locales los teneis solo vosotros

Es imprescindible que hagáis copias de seguridad de vuestros datos importantes

Los técnicos del SICUZ estamos a disposición para cualquier ayuda que necesiteis

Copias de Seguridad

Soportes:



Qué guardar:

La Regla del 3 – 2 – 1

- De cada archivo guardar **3** copias

  Disco de nuestro ordenador de trabajo

- Guardar **2** de ellas en soportes diferentes

  Un usb o disco externo (sin conexion permanente)

- Al menos **1** de ellas en un lugar externo

  Google Drive, Dropbox, etc…

Copia de seguridad en la nube

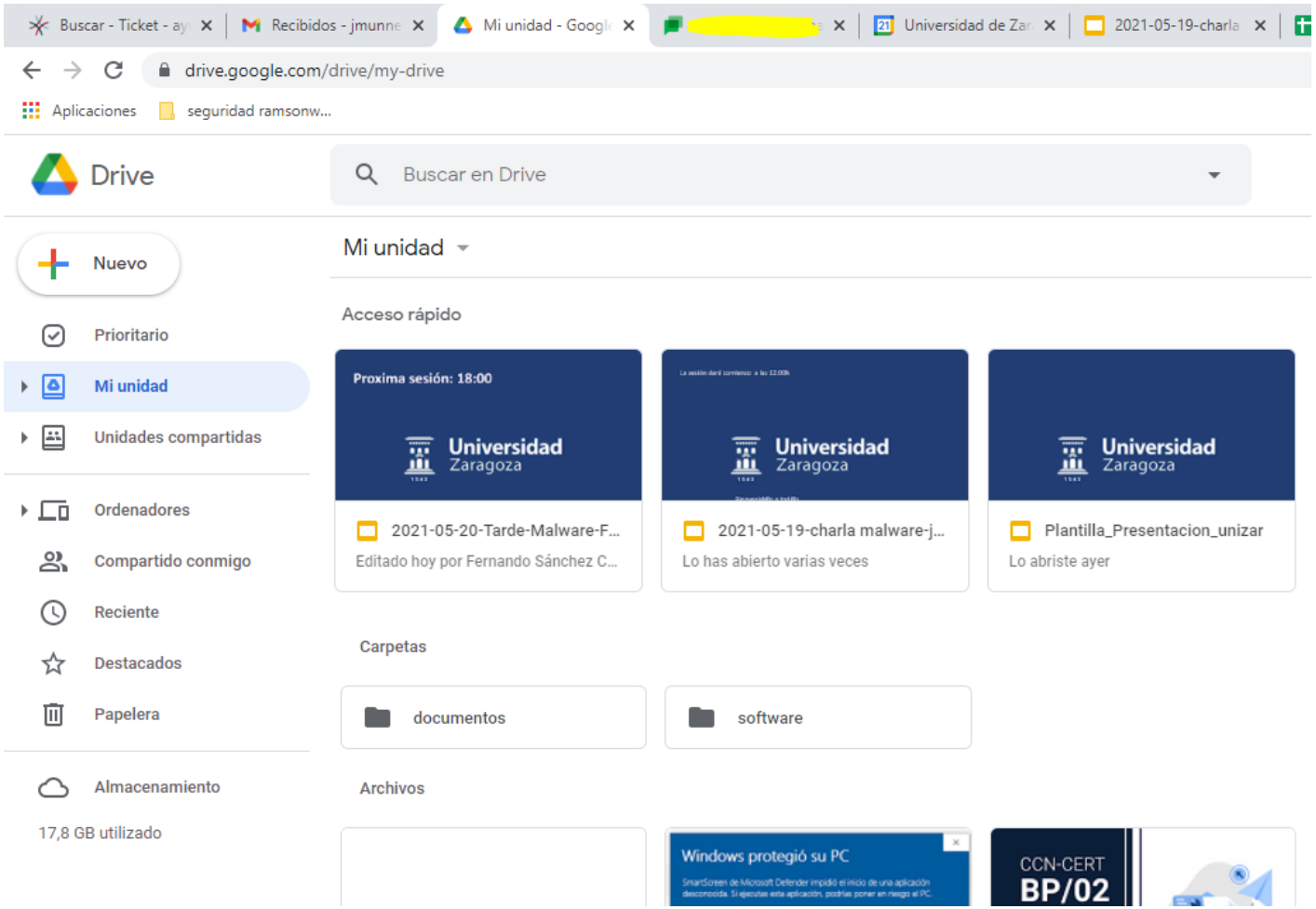
Google Drive, Dropbox o similar

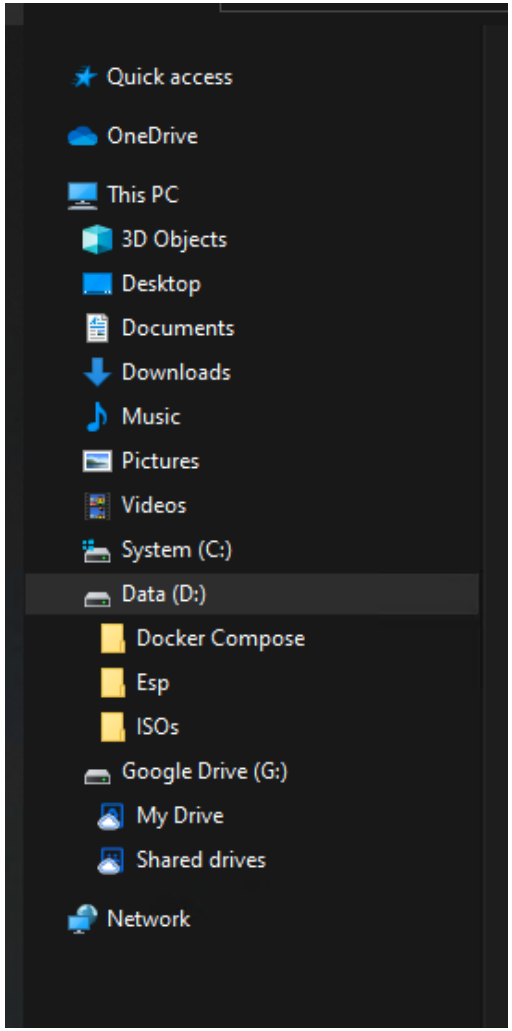
Desactivar la sincronización automática.
desinstalando el software que se instala por defecto con Google Drive o similar

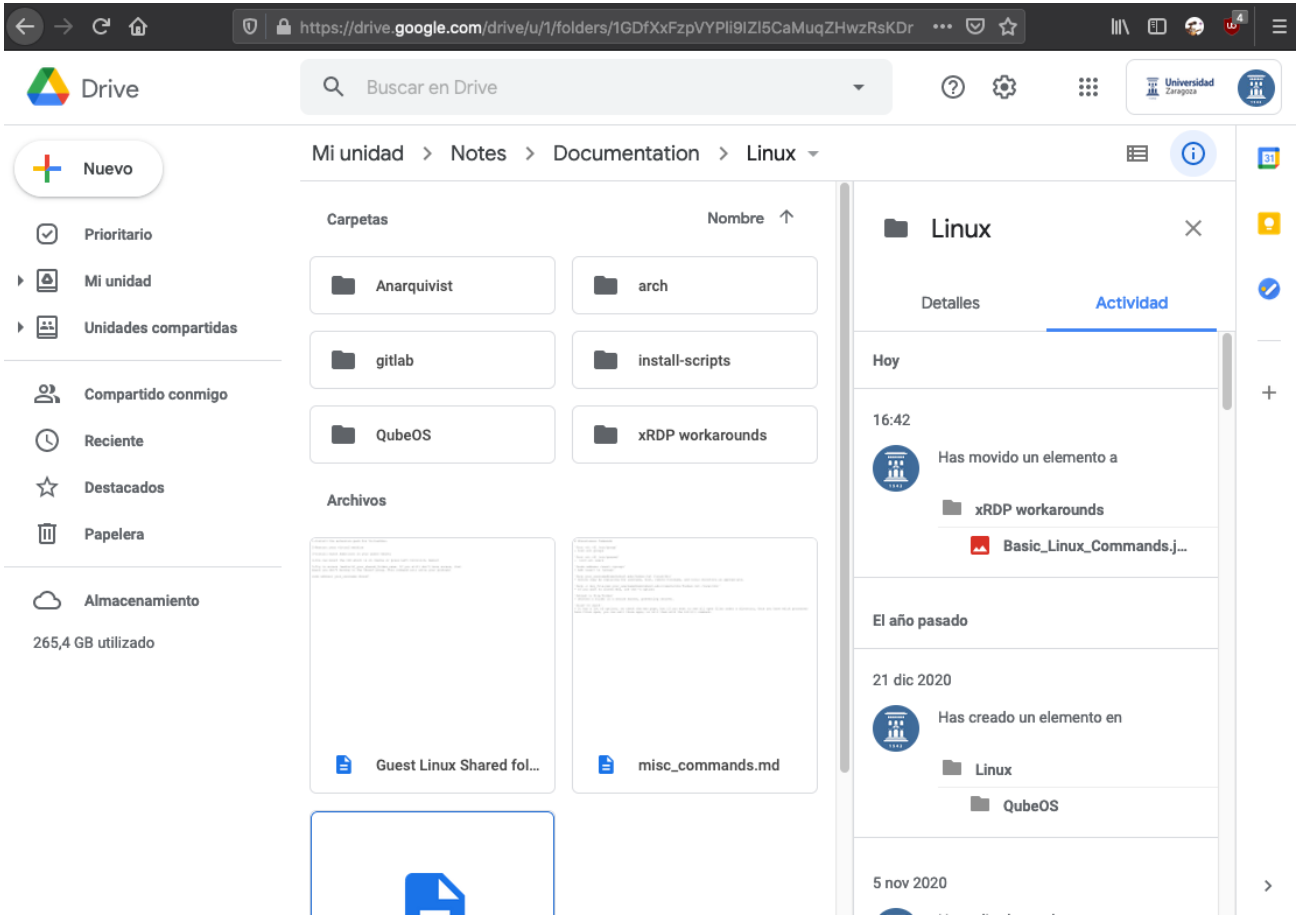
Conectarse puntualmente a la página web de Google Drive o Dropbox únicamente para hacer la copia

Así evitaremos que un posible ataque nos cifre los ficheros en la nube

Demo de copia a Google Drive utilizando su web




Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
System (C:)
Data (D:)
Docker Compose
Esp
ISOs
Google Drive (G:)
My Drive
Shared drives
Network


https://drive.google.com/drive/u/1/folders/1GDfXxFzpVYPli9IZl5CaMuqZHwzRsKDr
Drive
Buscar en Drive
Nuevo
Prioritario
Mi unidad
Unidades compartidas
Compartido conmigo
Reciente
Destacados
Papelera
Almacenamiento
265,4 GB utilizado
Mi unidad > Notes > Documentation > Linux
Carpetas
Nombre
Anarquivist
arch
gitlab
install-scripts
QubeOS
xRDP workarounds
Archivos
Guest Linux Shared fol...
misc_commands.md
Linux
Detalles
Actividad
Hoy
16:42
Has movido un elemento a
xRDP workarounds
Basic_Linux_Commands.j...
El año pasado
21 dic 2020
Has creado un elemento en
Linux
QubeOS
5 nov 2020

Copia de seguridad
en dispositivo USB

Conectar el dispositivo
Únicamente para hacer la copia
desenchufándolo después

Así evitaremos que un posible ataque de ransomware nos cifre la información del dispositivo USB

Confidencialidad de los datos

Al hacer una copia en un dispositivo externo USB, **corremos el riesgo de que caiga en manos de terceros** por pérdida o robo

Es importante cifrar la información o mantener el dispositivo bajo llave

Para cifrar los datos, el método recomendado es utilizar la aplicación libre 7Zip

Creando un archivo comprimido con contraseña y guardando en el dispositivo este archivo

En el Canal Herramientas TIC Unizar se encuentra disponible un vídeo que explica como cifrar y proteger en un archivo con contraseña una carpeta con el software 7Zip

Recordemos que una copia de seguridad no es tal hasta que has probado a restaurar o acceder al contenido de la misma

Resumen

Amenaza: **Ransomware**

Prevenir

buenas practicas

correo

emisor

mensaje

Mitigar

copia de seguridad

3-2-1

Varios soportes

Varias localizaciones

Más información:

sicuz.unizar.es/copias-seguridad