Servicio de
Informática
y Comunicaciones
Universidad Zaragoza

1542

Sesiones online ciberseguridad y cambio de contraseñas

30/03/2022

Propósito de esta charla

- Transmitir a la comunidad universitaria que existe un riesgo real de ciberataque a equipos de la Universidad de Zaragoza
- Informar a todos los usuarios de las medidas de prevención y protección frente a este tipo de amenazas.
- Destacar la recomendación de cambio de contraseñas como una medida necesaria para nuestra protección

Contenidos

- Situación actual y antecedentes de las amenazas de ciberataque
- Amenazas a la que nos enfrentamos: malware y ransomware
- Cómo se producen las infecciones por este tipo de virus.
- Medidas de prevención y de protección de nuestros equipos y datos
- Turno de preguntas
- Resumen: http://sicuz.unizar.es/contraseñas

Antecedentes

A lo largo de 2021 se han sucedido incidentes de este tipo contra organismos públicos como el SEPE, Telefónica y las Universidades de Córdoba, Castilla la Mancha y Autónoma de Barcelona.
En el caso de esta última, en Octubre de 2021, quedaron afectados gran parte de sus servicios corporativos, que tardaron varios meses en ser recuperados

Antecedentes

Universidad de Castilla-La Mancha
CAMPUS DE EXCELENCIA INTERNACIONAL

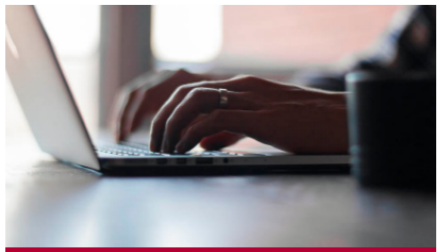
PREUNIVERSITARIO ESTUDIANTE EMPRESA English | Herramientas

UCLM ESTUDIOS INVESTIGACIÓN INNOVACIÓN INTERNACIONAL CULTURA

Inicio > La UCLM > Comunicación > Actualidad > La Universidad de Ca ..... ufrir un ciberataque

LA UCLM

- Institucional +
- Campus +
- Consejo de dirección +
- Órganos de Gobierno +
- Responsabilidad Social +
- Comunicación -
  - Identidad Visual Corporativa
  - Noticias
  - Previsiones
  - UCLM TV
- Servicios y gestión +
- Agenda +



Los equipos de la comunidad universitaria no se han visto afectados

Es una incidencia similar a la que ha afectado a otras universidades y entidades públicas

La Universidad de Castilla-La Mancha trabaja en la recuperación de los servicios digitales tras sufrir un ciberataque

19/04/2021

COMPARTIR:

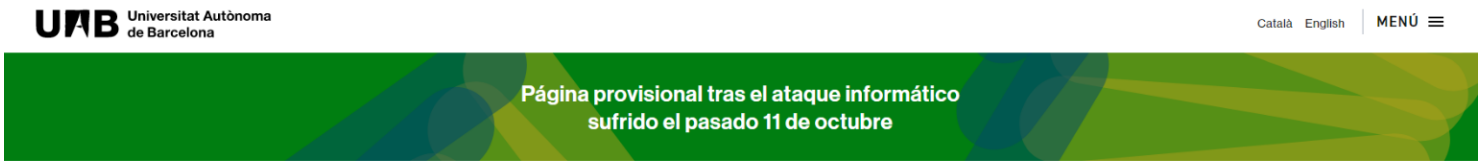
La Universidad de Castilla-La Mancha (UCLM) está trabajando en la recuperación de sus servicios digitales afectados por el ciberataque que sufrió la institución a las diez de la noche del domingo. La Universidad cortó inmediatamente la conectividad interna para amortiguar el alcance de la intrusión, del tipo ransomware.

Los profesionales del Área de Tecnología y Comunicaciones de la Universidad de Castilla-La Mancha (UCLM) están trabajando ininterrumpidamente para recuperar los servicios digitales afectados por un ciberataque producido en la noche de ayer, domingo. Se trata de un ataque de tipo ransomware como el que está afectando en los últimos meses a otras universidades españolas y extranjeras, y a otras instituciones públicas y privadas.

La UCLM ha denunciado el ataque al Centro Criptológico Nacional Computer Eemergency Response Team (CNN-CERT), el organismo encargado de velar por la ciberseguridad de la administración y los organismos públicos y las empresas estratégicas del país.
El Área TIC está evaluando la incidencia del ataque, aunque no hay evidencias de que información sensible se haya visto comprometida. La Universidad pudo amortiguar en parte los efectos del ataque al cortar la conectividad externa en cuanto se detectó la intrusión.

Gabinete Comunicación UCLM. Ciudad Real, 19 de abril de 2021

Antecedentes



AVISOS

11/10/2021. La Universitat Autònoma de Barcelona ha sufrido un ataque informático de origen desconocido.

25 de octubre de 2021

El ataque ha afectado, esencialmente, el sistema de virtualización que aloja una gran parte de los servicios corporativos. Esta afectación implica que no se podrán utilizar estos servicios y aplicativos.

Desde la Dirección de Tecnologies de la Informació i la Comunicació de la UAB se ha actuado siguiendo el protocolo establecido para estos casos, por un lado, aislando las máquinas infectadas, y por otro lado, aplicando medidas preventivas para evitar la propagación a sistemas no afectados.

Una vez se haya determinado en detalle los mecanismos de este ataque, se procederá a restablecer el sistema de forma escalonada, garantizando la integridad de los servicios que se vayan recuperando.

Durante esta semana se trabajará sin la utilización de ordenadores conectados a la red. Esto afectará a todos los ámbitos de actividad: docencia, investigación y administración.

Situación actual

El Gobierno alerta de ciberataques contra servicios vitales del Estado

- Llama a reforzar los protocolos a empresas de sectores críticos por posibles represalias por el apoyo a Kyiv
- Ya se ha detectado un ciberataque consistente en un defacement en los sistemas de una institución estatal sin "impacto significativo"

Aumentan las amenazas

Los expertos anticipan ciberataques en España tras la invasión: "Van a llegar"

Desde UNIR aseguran que es "muy complicado" colaborar con las autoridades rusas para perseguir este tipo de delito, porque según argumentan, el cibercrimen es una fuente de recursos financieros para el país.

- Zelenski denuncia la destrucción de un aeropuerto por el impacto de 8 misiles
- EEUU lanza un fondo de 2.500 millones para los países con planes de refugiados

LA INFORMACIÓN NOTICIA
06.03.2022 · 15:35h

Amenazas a las que nos enfrentamos:

Malware

Malware es un término genérico utilizado para describir una variedad de software: virus informáticos, gusanos, troyanos, spyware, publicidad no deseada, bulos, etc. que afectan a la privacidad y seguridad de nuestros equipos informáticos.

Amenazas a las que nos enfrentamos:

Ransomware

Ransomware o 'secuestro de datos', es un tipo de programa dañino que encripta los archivos del ordenador y pide un rescate a cambio de descifrar y recuperar esos archivos

Amenazas a las que nos enfrentamos:

Ransomware

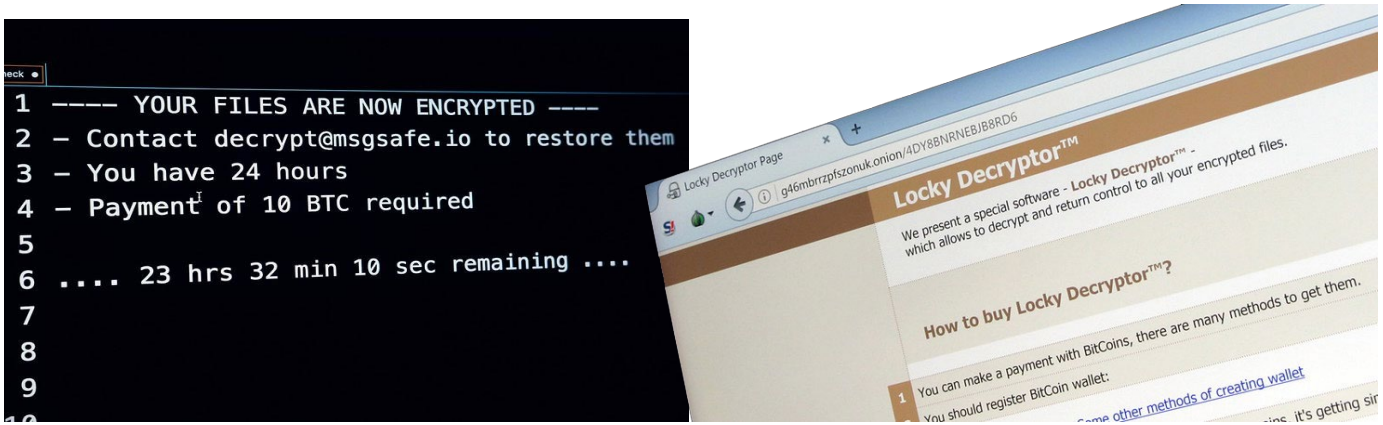
Ejemplos: Ryuk y **Pysa** son los nombres de las variantes detectadas en los ataques a las Universidades de Castilla la Mancha y Autónoma de Barcelona respectivamente.

- **Ryuk** infecta los ordenadores mediante correos electrónicos que introducen un troyano con la capacidad de analizar todo el tráfico de red y de robar credenciales de inicio de sesión.

- Los ataques de **Pysa** (“Protect Your System Amigo”) buscan obtener acceso a los sistemas generalmente mediante correos electrónicos con phishing y ataques contra sistemas que utilizan el protocolo de Escritorio Remoto.

Consecuencias de un ataque Ransomware

- Cifrado de los archivos locales o de unidades de red en carpetas compartidas mediante una clave criptográfica.
- Escaneo de la red para afectar a otros equipos y así seguir replicándose. En el caso de los ciberataques a las universidades anteriormente mencionadas, la infección alcanzó a los servicios corporativos.
- Petición de un rescate económico en criptomonedas para poder descifrarlos.



Consecuencias de un ataque Ransomware

Menú

El Confidencial

Iniciar sesión

Tecnología

"ESTÁN DESBORDADOS"

Chantaje al Ministerio de Trabajo: exigen un rescate para liberar los sistemas atacados

El Ministerio de Trabajo lo ha negado en todo momento, pero ha ocurrido: los cibercriminales exigen un rescate para liberar los sistemas secuestrados tras el ciberataque con el 'ransomware' Ryuk

Sede del Ministerio de Trabajo.

Cómo se producen las infecciones de Malware:

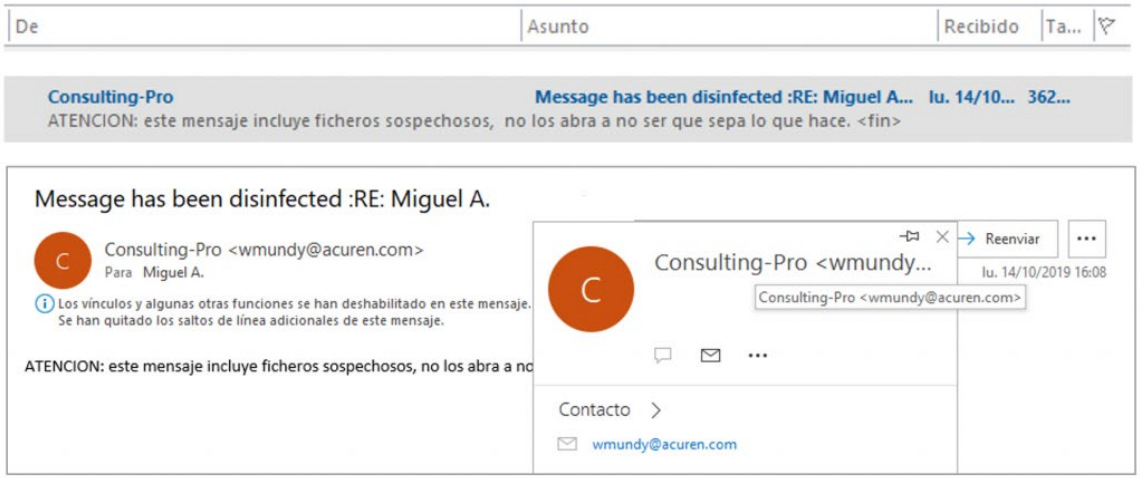
Suplantación de identidad: phising

Cómo se producen las infecciones de Malware:

Correos maliciosos

Mediante envíos de correos con remitente falso con el objetivo de enviar spam, difundir malware, llevar a cabo ataques de phishing y suplantar la identidad de personas.

Debemos prestar especial atención a los archivos adjuntos que contengan estos mensajes, y en el caso de que no tengamos claro si el documento es legítimo o no, lo mejor es no abrirlo.

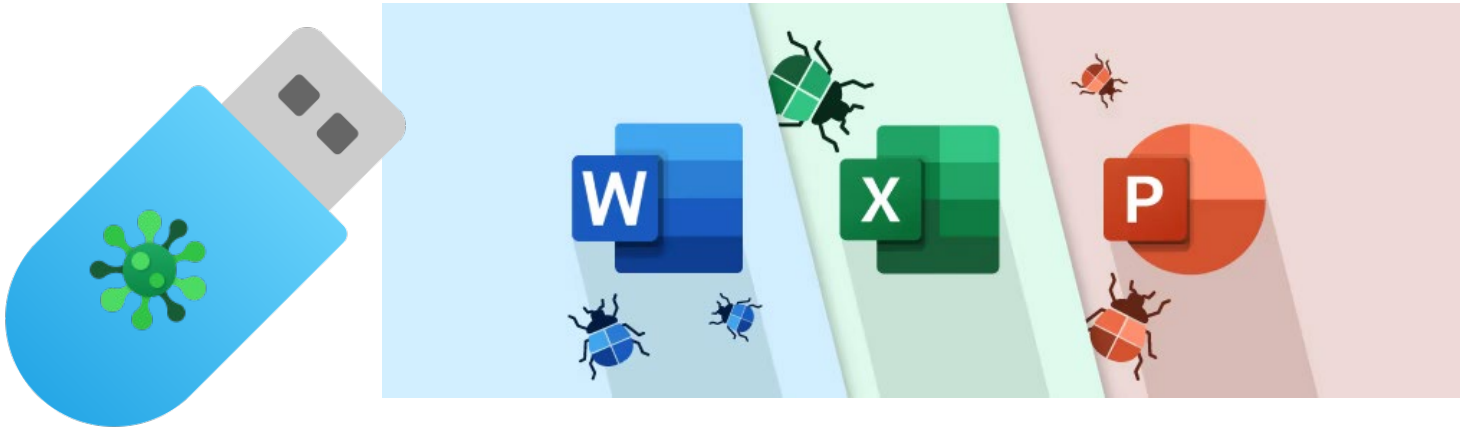


Cómo se producen las infecciones de Malware:

Dispositivos USB, Virus de macros

- **Dispositivos de almacenamiento USB infectados**
- **Macros de Office**

  Un virus de macro es un tipo de virus informático que podría almacenarse en macros (tareas automatizadas) dentro de un archivo de Microsoft Office (como un documento, una presentación, un libro o una plantilla)



Acciones preventivas por parte del Servicio de Informática y Comunicaciones

- Medidas de refuerzo de copias de seguridad de los datos corporativos.
- Actualizaciones y parches de seguridad en servidores corporativos
- Refuerzo en la seguridad de las comunicaciones y los accesos.
- Monitorización del tráfico de red y alertas.
- Despliegue de vacunas contra Ramsonware
- Charlas de concienciación frente a riesgo de ciberataque

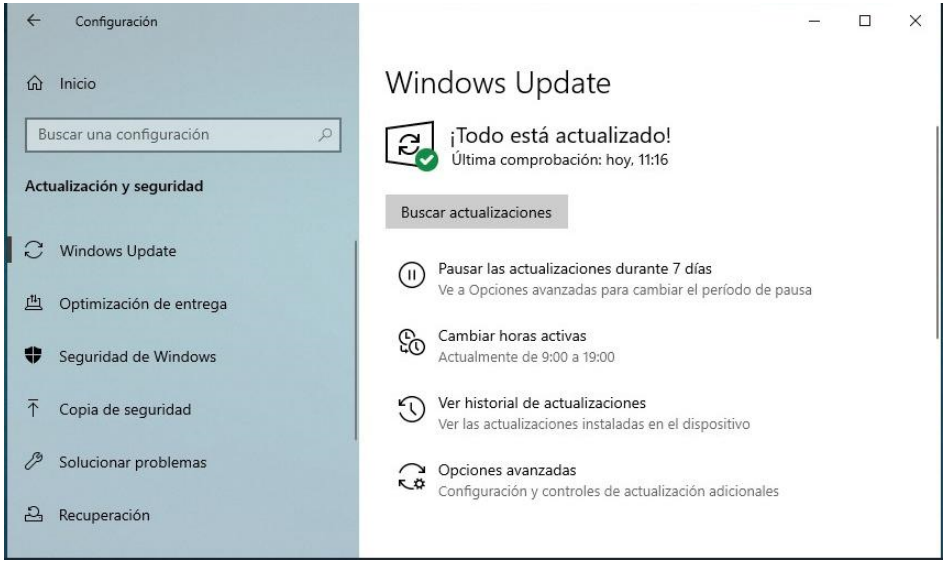
Correos no solicitados, enlaces y contraseñas

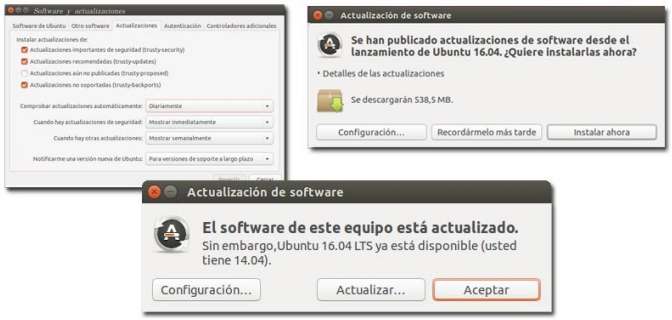
- **Evitar abrir y contestar correos de usuarios desconocidos** sin que lo hayamos solicitado y eliminarlos directamente.
- **Revisar los enlaces** antes de hacer clic **y desconfiar de los ficheros adjuntos** aunque sean de contactos conocidos
- **Utilizar contraseñas robustas** y en la medida de lo posible no utilizar cuentas con permisos de administrador en el equipo.

Medidas de prevención por parte de los usuarios

Actualizaciones sistema operativo

Es muy importante que nuestro **sistema operativo esté actualizado**, ya que con ello obtendremos soluciones a problemas de seguridad y vulnerabilidad de los equipos.

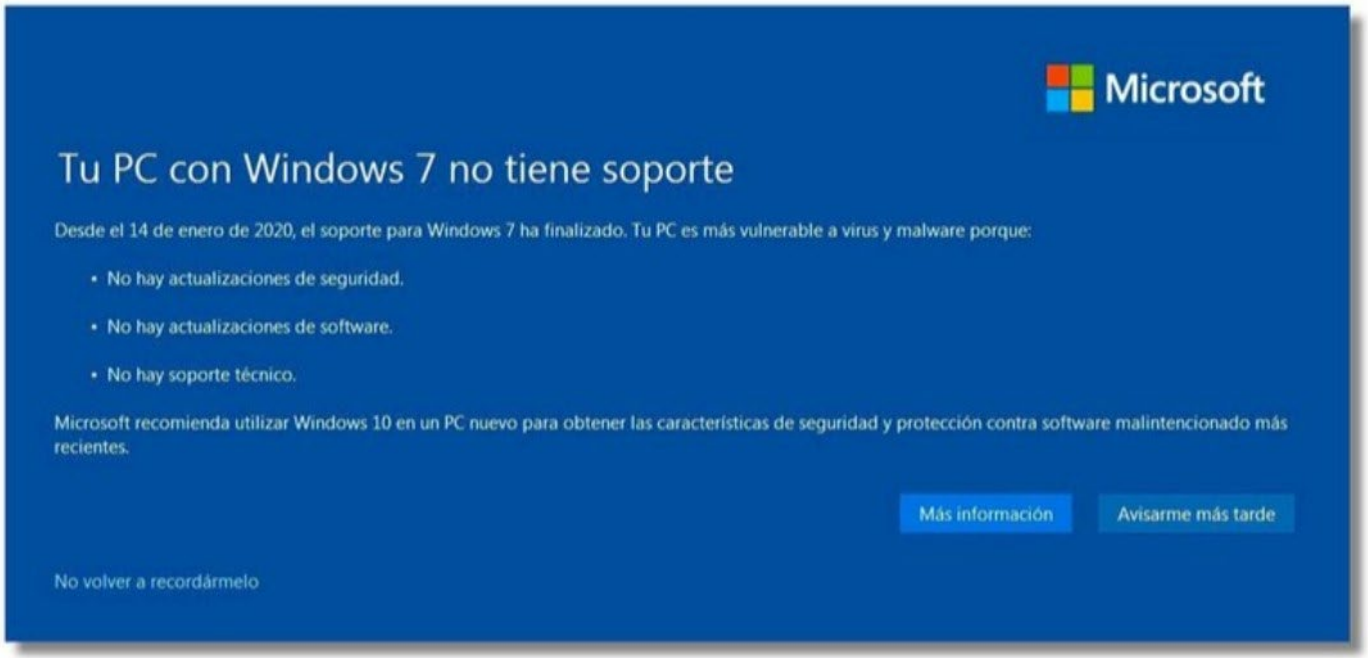




Medidas de prevención por parte de los usuarios

Actualizaciones sistema operativo

Desaconsejamos el uso en equipos conectados a la red de la Universidad de Zaragoza de sistemas operativos cuyo ciclo de soporte ha terminado, y por tanto ya no reciben actualizaciones de seguridad, como en el caso de Windows 7 y sistemas anteriores.

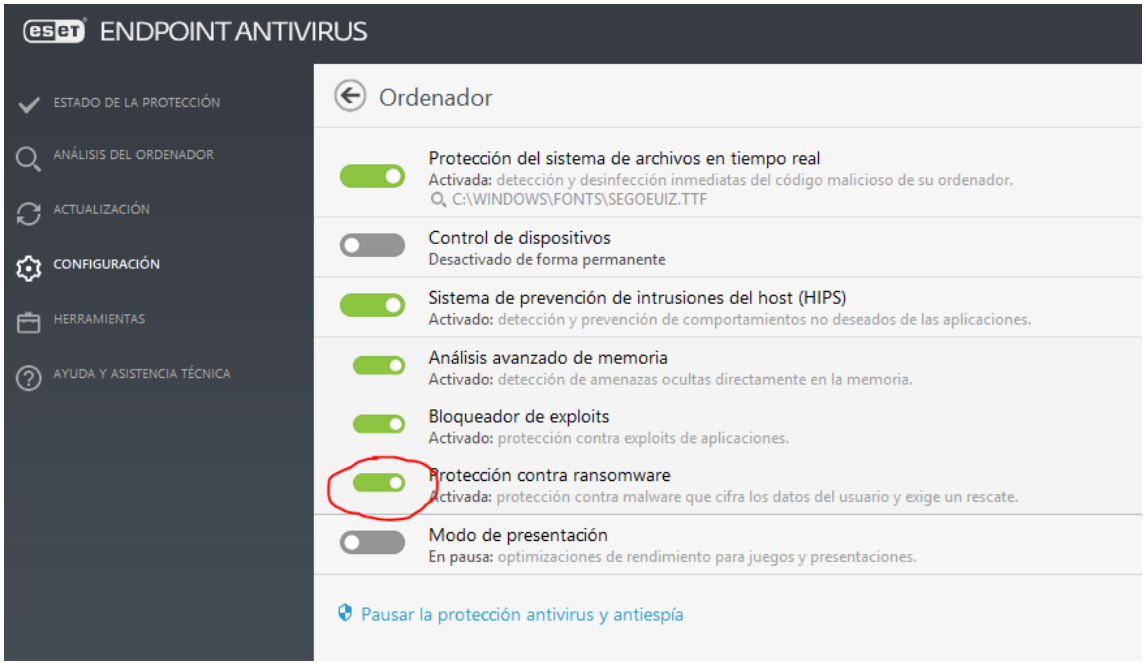


Medidas de prevención por parte de los usuarios

Uso del antivirus corporativo

Tener instalada la última versión de **ESET Antivirus** (v8) disponible en Unizar (licencia disponible sólo en equipos propiedad de la universidad).

La instalación, configuración y actualizaciones se realizan de manera automática.



Medidas de prevención por parte de los usuarios

Instalación de microCLAUDIA

microCLAUDIA es un sistema de vacunas contra *ransomware*, desarrollado por el CERT del Centro Criptológico Nacional que se instala en los equipos Windows de los usuarios.

En la página https://sicuz.unizar.es/microCLAUDIA encontraremos mas información e instrucciones para instalar en nuestro equipo de trabajo.

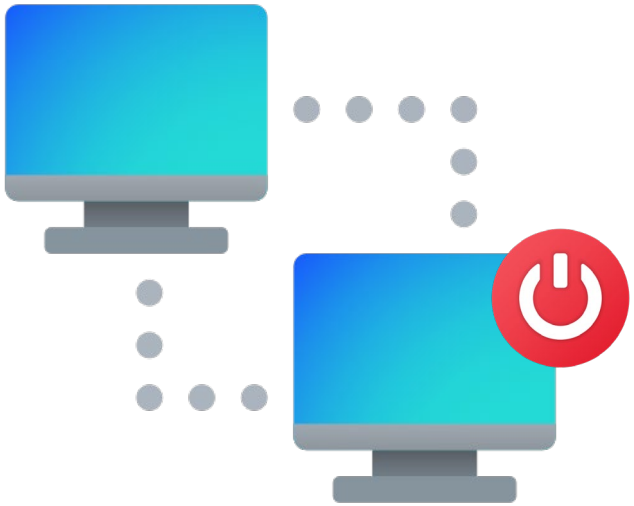
Realización periódica de copias de seguridad

Es de vital importancia realizar copias de seguridad de los datos importantes que tenemos en nuestro ordenador de trabajo para poderlos recuperar en el caso de que hayamos sido afectados por un ataque de este tipo.

En la página https://sicuz.unizar.es/copias-seguridad encontraremos mas información de como realizar nuestras copias de seguridad.

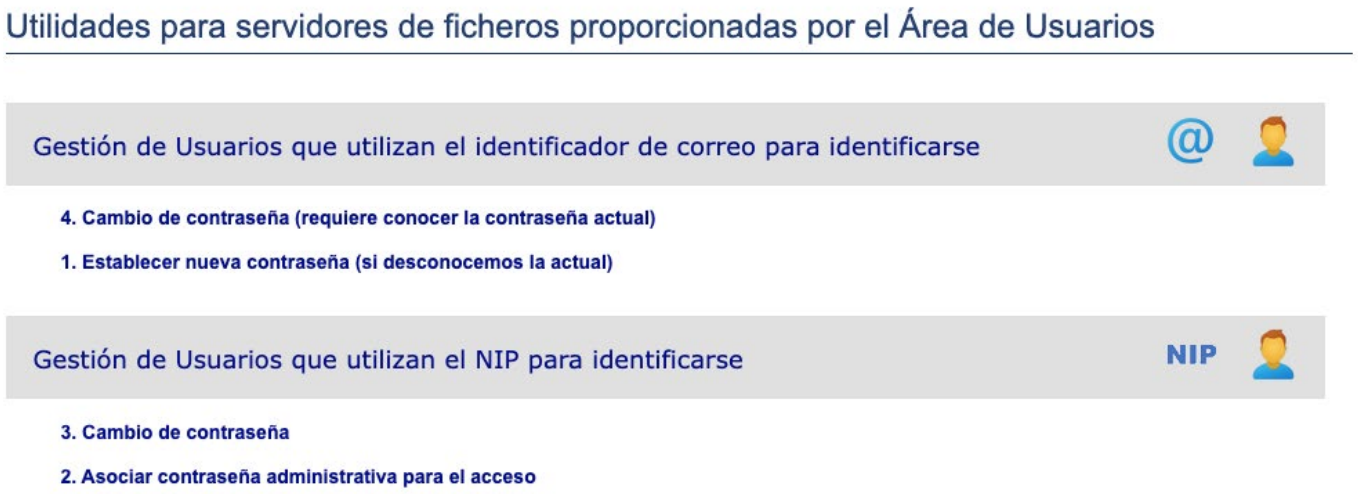
Recomendaciones de apagado de los equipos

Recomendamos el apagado de nuestros equipos de trabajo cuando no sea necesario el acceso a ellos, de esta manera evitaremos el riesgo que suponen para las amenazas de ciberataque los equipos que permanecen encendidos y conectados a la red.



Cambio de contraseña en servidores de ficheros (psfunizar)

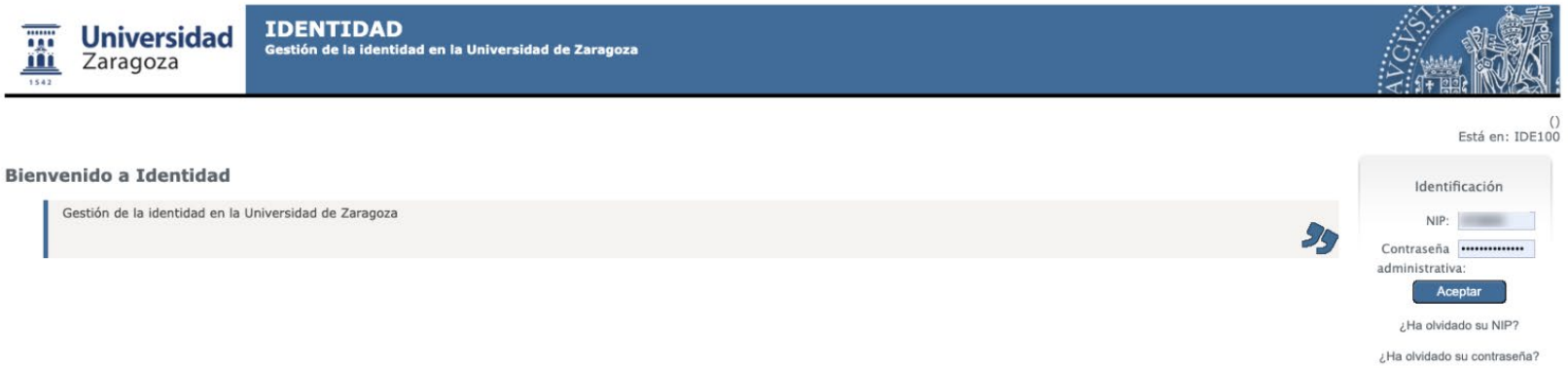
Para cambiar la contraseña deberemos utilizar las Utilidades de Gestión de Usuarios, seleccionando la opción correspondiente:
https://ausuarios.unizar.es/psfs/index.html
Posteriormente, en nuestro equipo tendremos que reconectar/cambiar las credenciales de conexión al servidor de ficheros.



Medidas de prevención por parte de los usuarios

Cambio de la contraseña administrativa

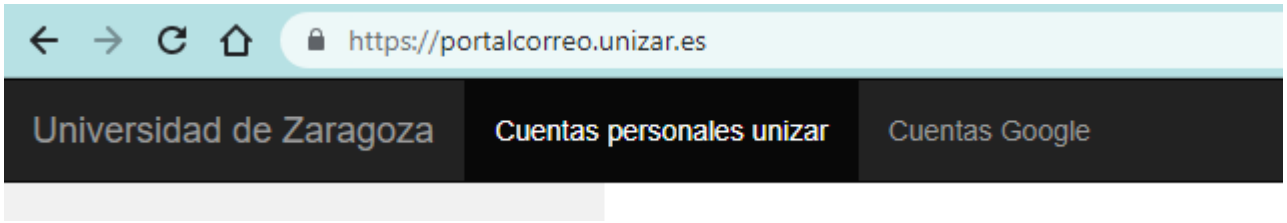
De esta manera evitamos que los ataques de ransomware accedan a la vpn a través de contraseñas con la seguridad comprometida. Para cambiar nuestra contraseña deberemos acceder a identidad.unizar.es



Medidas de prevención por parte de los usuarios

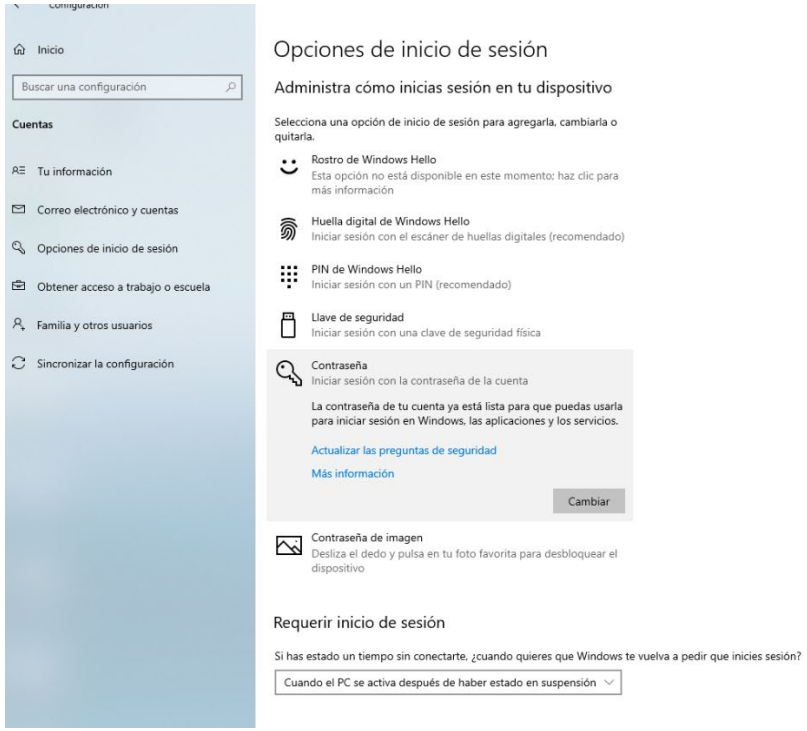
Cambio de la contraseña de correo

Para cambiar las contraseñas de nuestra cuenta de correo unizar y de las cuentas vinculadas a Google, deberemos acceder a portalcorreo.unizar.es



Cambio de la contraseña de inicio de sesión en el equipo

En Windows 10 a través de Configuración > Cuentas > Opciones de inicio de sesión



Medidas de prevención por parte de los usuarios

Recomendaciones sobre contraseñas

Recomendaciones sobre contraseñas

- No usar la misma contraseña que ya teníamos.
- Debe tener una longitud de más de 8 caracteres.
- Emplear una combinación de letras, números, mayúsculas y símbolos para formar una cadena de caracteres que no se asemejen a palabras o nombres.
- No deben utilizarse en ningún caso palabras de diccionario, nombres propios o fechas significativas.
- Una contraseña segura debe ser única para cada cuenta a fin de reducir su vulnerabilidad.

Desaconsejamos el uso de gestores de contraseñas para almacenar nuestros datos de acceso a los diferentes recursos de la Universidad de Zaragoza

Muchas gracias por su atención

Si necesita ayuda acerca de alguna de las cuestiones que hemos planteado, puede contactar con el Servicio de Informática y Comunicaciones a través del personal técnico de su Centro o a través de un ticket de soporte en Ayudica.

Turno de preguntas