Antecedentes

Desde 1988, cada 30 de noviembre, se celebra el **Día Internacional de la Seguridad de la Información** (*Computer Security Day)*. Es una iniciativa de la *Association for Computing Machinery* (ACM) en la que se invita a la comunidad a contribuir en la adopción de una cultura de seguridad de la información.

Mitos

- La protección es un tema técnico y compete al área de Sistemas o de TI.
- La información que tengo/uso no tiene valor.
- No me afecta perder información.
- A mi no me va a suceder.

La seguridad de la información **no es** 100% eficaz.

No todo es lo que parece.

Malware, amenaza entre nosotros

El Usuario

El Dispositivo

El *Malware*

La **Ingeniería Social** utiliza el *malware* para llegar al usuario.

Encuesta

¿Instalas aplicaciones en tu dispositivo (laptop, teléfono, etc.)?
95% contestó que sí.

Al usar Apps, ¿autorizas acceso a ubicación, documentos o fotos?
55% contestó que sí.

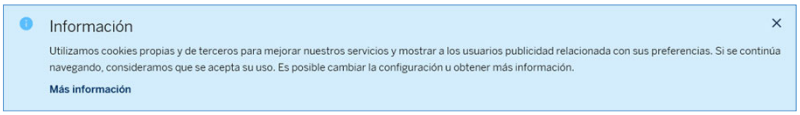
¿Cuál es la frecuencia de uso de las Apps instaladas en tu dispositivo inteligente (teléfono celular, por ejemplo)?
50% al menos 15 veces por semana.
40% a lo más 5 veces por semana.
10% una vez por mes.

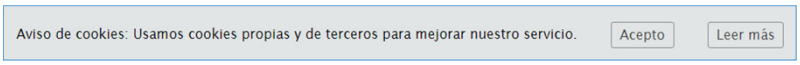
¿Has perdido información a causa de un incidente con malware?
15% contesto que sí.

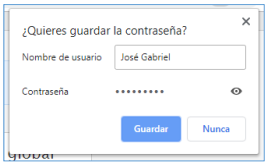
Gracias a los asistentes que colaboraron.

UX nos hace vulnerables

- Usabilidad.
- Cookies.
- Metadatos.
- Gestión de contraseñas.
- APPs acceden a:
  - Ubicación (GPS)
  - Fotografías
  - Formas de pago
  - Credenciales de acceso







UX – Experiencia de Usuario. **Cookies** – Registran actividad del usuario. **CC BY-NC-S**

- Las cosas tienen Internet.
- Las comunicaciones son más sofisticadas.
- Las tareas se hacen con mayor facilidad en los dispositivos inteligentes.
- Los servicios se han digitalizado.
- Los costos han disminuido.

Todo está conectado. **CC BY-NC-S**

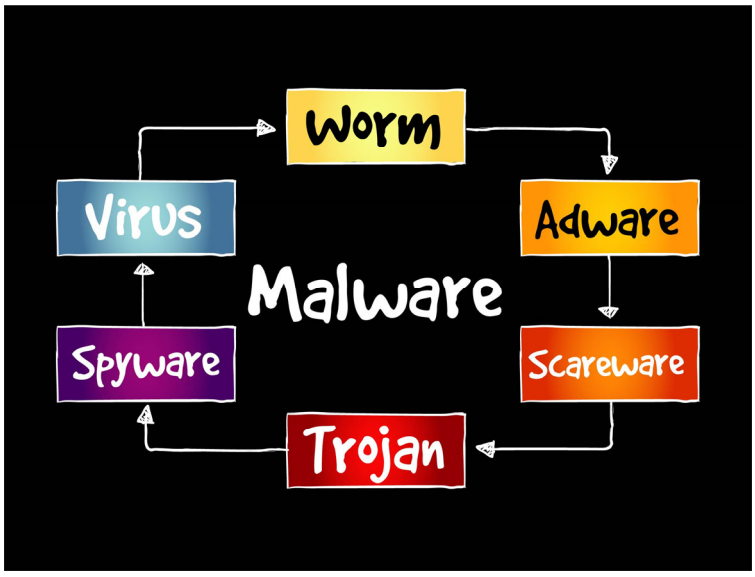
- Delincuencia organizada.
- Es un negocio, el rescate se paga en criptomonedas.
- Afecta organizaciones y usuarios.
- Aprovecha los avances tecnológicos.

El secuestro de información ya es común.

Malware

Software malicioso diseñado para afectar un dispositivo para infiltrarse en ella o acceder a la información.

- Software y Apps
- Archivos
- Imágenes
- Correos electrónicos
- Links
- Scripts



El **ramsomware** es el más conocido en la actualidad.

Un ciberataque deja sin servicio a la UAB

14 octubre, 2021 Por Javier Aranda — 1 comentario

La madrugada del pasado lunes, la **Universitat Autònoma de Barcelona (UAB)** sufrió un ciberataque en su infraestructura digital, obligando a cancelar algunas clases clases virtuales.

Universitat Autònoma de Barcelona

A **primera hora** del lunes 11 de octubre saltaban las alarmas en la Universitat Autònoma de Barcelona. Un ciberataque habría afectado a los servidores centrales de la universidad. Fuentes de la UAB afirman que, debido a la naturaleza de estos ataques, es **muy complicado determinar su origen**, aunque se está llevando a cabo una investigación. A falta de confirmación oficial, parece apuntar a un ataque de tipo **ransomware**. Tras las primeras evaluaciones de daños, **las bases de datos corporativas no se habrían visto afectadas**,

Aranda, Javier. (2021). Un ciberataque deja sin servicio a la UAB. Noviembre 27, 2021, de Hispasec Sitio web: https://unaaldia.hispasec.com/2021/10/un-ciberataque-deja-sin-servicio-a-la-uab.html

La UAB iba a tardar "días" en recuperarse del ciberataque de ransomware... ahora la expectativa es hacerlo a las puertas de 2022

22 Octubre 2021

1 Comentario

MARCOS MERINO

@MarcosMerino_B

Merino, Marcos. (2021). La UAB iba a tardar "días" en recuperarse del ciberataque de ransomware… ahora la expectativa es hacerlo a las puertas de 2022. Noviembre 27, 2021, de Genbeta Sitio web: https://www.genbeta.com/actualidad/uab-iba-a-tardar-dias-recuperarse-ciberataque-ransomware-ahora-expectativa-hacerlo-a-puertas-2022

Las Universidades también están expuestas.

Las amenazas no descansan

Desinformación

Robo de Identidad

Hackers

Ingeniería Social

Haz Equipo

- ✓ **Actúa** con calma
- ✓ **Verifica** la procedencia
- ✓ **Consulta** las plataformas oficiales
- ✓ **Sigue** las recomendaciones de las instancias autorizadas

La información hace diferencia CC BY-NC-S

¿Qué debo hacer?

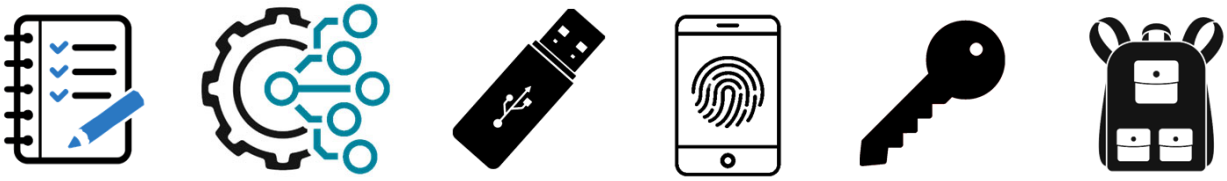
MESA DE SERVICIOS DTI

- Validar antes de actuar. Ante la duda, la pregunta.
- Identificar la información que poseo, establecer criterios o verificar si existe alguno en la institución.
- Establecer un ciclo de vida para la información.
- Elaborar respaldos periódicos de información, verificarlos.
- Permitir la actualización de software y aplicaciones.
- Utilizar contraseñas en combinación con un *segundo factor*.

Segundo Factor = contraseña + (verificación vía correo). CC BY-NC-S

Adopta una cultura de autoprotección

- ✓ **Identifica** la información vital
- ✓ **Resguarda** en versión digital
- ✓ **Actualiza** con oportunidad
- ✓ **Utiliza** mecanismos de seguridad



Mejor se protege, el que se previene CC BY-NC-S

La concienciación busca …

- **Potenciar** las habilidades de los usuarios.
- **Mantener** una higiene digital.
- **Promover** una cultura de prevención.
- **Difundir** una postura de autoprotección.
- **Informar** a la comunidad.

Todos podemos contribuir. ***PASA LA VOZ*** CC BY-NC-S

GRACIAS

Casa abierta al tiempo

seguridad@correo.uam.mx