Universitat de les Illes Balears

Cómo acercar la Ciberseguridad a la comunidad universitaria

Maribel Barceló

29/05/2024

52


Ciberconsells
UIB
AMB
TU
+SEGURS

Ciberconsells

UIB

CONTIGO

+SEGUROS

Objetivo

Concienciar en ciberseguridad a la comunidad universitaria

Proporcionar a la comunidad de la UIB información y recursos sobre ciberseguridad

Herramientas

Presentar información y recursos a través de la web de seguridad

Confluence

Wiki para trabajar colaborativamente

Universitat de les Illes Balears

MomentUIB

Boletín de noticias UIB

Universitat de les Illes Balears | PORTAL el meu espai personal

Portal personal UIB

Web Seguridad TI

https://seguretat.uib.es

uib.cat

Web Seguridad TI

https://seguretat.uib.es

uib.cat

Perfiles necesarios

- Técnicos de TIC
- Periodistas
- Diseñadores gráficos
- Traductores

Equipo del proyecto

Servicio de Infraestructuras TIC (SITIC)

Coordinación

Servicio de Comunicación (COM)

Servicio de Identidad y Cultura Institucional (SICI)

Servicio Lingüístico (SLG)

UIB Universitat de les Illes Balears

Creación de un espacio en wiki Confluence

- Para compartir información y colaborar en el proyecto fácilmente.
- Crear y editar páginas con todo el equipo en tiempo real o de forma asíncrona.
- Recopilar comentarios o entablar conversaciones sin problemas con los comentarios insertados.
- Notificar las actualizaciones a los miembros del equipo con @menciones.

Planificación

- Establecer un calendario con la información que se quiere difundir cada semana.

2023

Proposta ordre publicació

Data	Id creació	Estat	Categoria	Títol
18-ene-2023	20	PUBLICAT	Contrasenyes	20. Ciberconsell 20: CON-002 Canviar les contrasenyes que venen per defecte en els dispositius o aplicacions!
25-ene-2023	21	PUBLICAT	Correu electrònic	21. Ciberconsell 21: MAI-007 Comprovar l'extensió dels fitxers que vols descarregar!
01-feb-2023	22	PUBLICAT	Navegació web	22. Ciberconsell 22: NAV-0005 Utilitzar navegació privada quan es navega per Internet des de dispositius que no són nostros!
08-feb-2023	23	PUBLICAT	Lloc de feina	23. Ciberconsell 23: LFE-006 Notifica qualsevol incidència de seguretat!
15-feb-2023	24	PUBLICAT	WIFI	24. Ciberconsell 24: WIFI-002 Evita connectar-te automàticament a xarxes Wi-Fi que no siguin de confiança!
22-feb-2023	25	PUBLICAT	Xarxes socials	25. Ciberconsell 25: XSO-002 Crea una contrasenya segura i diferent per a cada xarxa social!
08-mar-2023	26	PUBLICAT	Navegació web	26. Ciberconsell 26: NAV-0006 No emmagatzemar al navegador credencials d'accés a serveis web!
15-mar-2023	27	PUBLICAT	Lloc de feina	27. Ciberconsell 27: LFE-007 No instal·lar aplicacions sense llicència o l'origen de les quals desconeguis!
22-mar-2023	28	PUBLICAT	Xarxes socials	28. Ciberconsell 28: XSO-003 Determina quins continguts podran veure els altres usuaris i quina interacció els permets!
29-mar-2023	29	PUBLICAT	WIFI	29. Ciberconsell 29: WIFI-003 No intercanviïs informació privada quan et connectis a una xarxa wifi pública o poc fiable!

Workflow

1. Ideas del mensaje que se quiere transmitir con enlaces a fuentes de información relacionadas

Servicio de Infraestructuras TIC (SITIC)

Técnico que prepara la información de la que se quiere concienciar y trabaja con los servicios para obtener un resultado final y publicarlo en la web

Workflow

Preparación | **Redacción** | Validación | Diseño | Traducción | Difusión

AMB TU +SEGURS
CiberconsellUIB

2. Poner título impactante y redacta el mensaje

Servicio de Comunicación (COM)

Persona que facilita la comprensión lectora con el lenguaje específico de ciberseguridad

ESPAÑOL

Título: ¿Cómo puedo saber si mis datos se han filtrado en internet?

En caso de sospecha o solo como verificación de control, existen servicios que pueden ayudarnos a saber si nuestros datos han sido expuestas a un filtración y, por lo tanto, su seguridad puede estar comprometida.

Uno de estos servicios es **Have I Been Pwned**, que recopila información de 670 sitios web que han sido afectados por una brecha y de más de 12.500 millones de cuentas expuestas. Basta poner nuestra dirección de correo o el número de teléfono y nos dirá si nuestra cuenta ha sido comprometida. Recuerda que es responsabilidad de cada uno utilizar contraseñas seguras y cambiarlas en caso de sufrir un incidente de seguridad. Comprueba en el siguiente enlace la seguridad de tus datos:

https://haveibeenpwned.com/

Más información

- Cómo saber si te han hackeado el correo
- Cómo funciona comprobar si te han robado las contraseñas

Workflow

Preparación | Redacción | **Validación** | Diseño | Traducción | Difusión

3. Comprobación de que el mensaje es correcto desde el punto de vista técnico

Servicio de Infraestructuras TIC (SITIC)

Técnico que realiza la revisión del título y texto propuesto. Además, realiza la comprobación de coherencia desde el punto de vista técnico.

Workflow

Preparación | Redacción | Validación | **Diseño** | Traducción | Difusión

4. Diseño de la imagen que representa el mensaje

Servicio de Identidad y Cultura Institucional (SICI)

Persona que diseña las imágenes para trasmitir el mensaje de manera gráfica.

Acciones a realizar para evitar el peligro

Acciones a realizar para estar protegidos

Workflow

Preparación → Redacción → Validación → Diseño → **Traducción** → Difusión

5. Traducción del mensaje y la imagen en catalán

Servicio Lingüístico (SLG)

Persona que revisa y normaliza al catalán, lengua oficial en la Universidad.

CATALÀ

Títol: Com puc saber si les meves dades s'han filtrat a internet?

En cas de sospita o només com a verificació de control, hi ha serveis que poden ajudar-nos a saber si les nostres dades han estat exposades a una filtració i si, per tant, la seguretat pot estar compromesa.

Un d'aquests serveis és **Have I Been Pwned**, que recopila informació de 670 llocs web que han estat afectats per una bretxa, així com de més de 12.500 milions de comptes exposats. Basta posar la nostra direcció de correu o el número de telèfon i ens dirà si el nostre compte ha estat compromès. Recorda que és responsabilitat de cada persona utilitzar contrasenyes segures i canviar-les en cas de sofrir un incident de seguretat. Comprova la seguretat de les teves dades a l'enllaç següent:

https://haveibeenpwned.com/

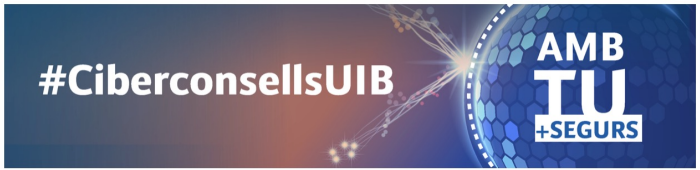
Més informació

- Com saber si han vulnerat el teu compte de correu electrònic
- Com funciona comprovar si t'han robat contrasenyes

Workflow

Preparación → Redacción → Validación → Diseño → Traducción → **Difusión**

6. Difusión del mensaje



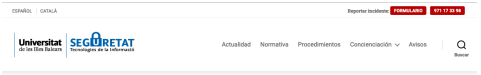
Com puc saber si les meves dades s'han filtrat a internet?

En cas de sospita o només com a verificació de control, hi ha serveis que poden ajudar-nos a saber si les nostres dades han estat exposades a una filtració i si, per tant, la seguretat pot estar compromesa.

Un d'aquests serveis és Have I Been Pwned, que recopila informació de 670 llocs web que han estat afectats per una bretxa, així com de més de 12.500 milions de comptes exposats. Basta posar la nostra direcció de correu o el número de telèfon i ens dirà si el nostre compte ha estat compromès.

SABER-NE MÉS COMPARTEIX

Boletín semanal UIB



CIBERCONSEJO

#33. ¿Cómo puedo saber si mis datos se han filtrado en internet?

10 de mayo de 2023

En caso de sospecha o solo como verificación de control, existen servicios que pueden ayudarnos a saber si nuestros datos han sido expuestas a un filtración y, por lo tanto, su seguridad puede estar comprometida.

Uno de estos servicios es *Have I Been Pwned*, que recopila información de 670 sitios web que han sido afectados por una brecha y de más de 12.500 millones de cuentas expuestas. Basta poner nuestra dirección de correo o el número de teléfono y nos dirá si nuestra cuenta ha sido comprometida. Recuerda que es responsabilidad de cada uno utilizar contraseñas seguras y cambiarlas en caso de sufrir un incidente de seguridad. Comprueba en el siguiente enlace la seguridad de tus datos:

Web Seguridad UIB

Ciberconsejos: Categorías

- Se ha elaborado un total de **52** ciberconsejos
- Clasificación

Contraseñas

Correo electrónico

Puesto de trabajo

Navegación web

Wi-Fi

Redes sociales

52

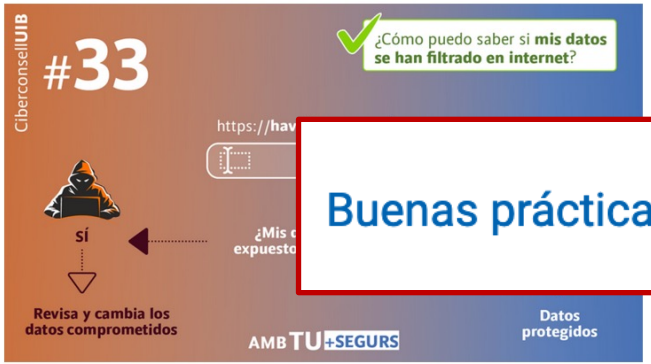

CiberconsellUIB
#4
Si el candado está cerrado y la web comienza por "HTTPS"
https://www.
Página no segura
Página segura
AMB TU +SEGURS
CiberconsellUIB
#3
Desconfia dels QR en solitari en llocs públics
AMB TU +SEGURS
CiberconsellUIB
#2
Sempre còpia oculta
CC
CCO/BCC
AMB TU +SEGURS
CiberconsellUIB
#7
No actualizado
AMB T

Ciberconsejos relacionados con Buenas prácticas

CIBERCONSEJO

#33. ¿Cómo puedo saber si mis datos se han filtrado en internet?

10 de mayo de 2023



Buenas prácticas en el uso del correo electrónico

En caso de sospecha o solo como verificación de control, existen servicios que pueden ayudarnos a saber si nuestros datos han sido expuestas a un filtración y, por lo tanto, su seguridad puede estar comprometida.

Uno de estos servicios es *Have I Been Pwned*, que recopila información de 670 sitios web que han sido afectados por una brecha y de más de 12.500 millones de cuentas expuestas. Basta poner nuestra dirección de correo o el número de teléfono y nos dirá si nuestra cuenta ha sido comprometida. Recuerda que es responsabilidad de cada uno utilizar contraseñas seguras y cambiarlas en caso de sufrir un incidente de seguridad. Comprueba en el siguiente enlace la seguridad de tus datos:

https://haveibeenpwned.com/

Más información:

- Cómo saber si te han hackeado el correo
- Cómo funciona comprobar si te han robado las contraseñas

Buenas prácticas en el uso del correo electrónico

Buenas prácticas

Selección de las categorías más relevantes que afectan a los usuarios

Buenas prácticas

- Resumen de los Informes de Buenas Prácticas del CCN-CERT del Centro Criptológico Nacional (CCN) en positivo y negativo
  - Correo electrónico
    - CCN-CERT BP/02 ‘Correo electrónico’ (Mayo 2021)
  - Navegación web
    - CCN-CERT BP/06 ‘Seguridad y riesgos de los navegadores web’ (Junio 2021)
  - Redes Sociales
    - CCN-CERT BP/08 ‘Redes Sociales’ (Julio 2021)

Buenas prácticas

- Información publicada en
  - INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE)
  - Oficina de Seguridad del Internatuta

- Información adicional de artículos, blogs, vídeos e infografías

Ejemplo: Buenas Prácticas Contraseñas

Recomendaciones y buenas prácticas de uso

- Antes de abrir cualquier fichero descargado desde el correo **asegurarse de cuál es su extensión** y no fiarse solo del icono asociado al fichero.
- Cuando se envía un mensaje a varias personas y se quiere evitar que los destinatarios puedan ver el resto de direcciones, **utilizar la función de copia oculta** (CCO o BCC).
- Utilizar **listas de distribución** cuando se tenga que hacer un **envío masivo de correos**.
- **Evitar hacer clic directamente en cualquier enlace desde el propio cliente de correo**. Si el enlace es desconocido es recomendable buscar información en motores de búsqueda como Google o Bing.
- **Cifrar los mensajes** de correo que contengan **información sensible**.

- **No abrir ningún enlace ni descargar ningún fichero adjunto** procedente de un correo electrónico que presente cualquier síntoma o patrón **fuera de lo que se considera «normal»** o habitual.
- **No fiarse únicamente del nombre del remitente**. Comprobar que el dominio del correo recibido (el que hay después de @ de la dirección) es de confianza. Si un correo procedente de un contacto conocido solicita información inusual, contactar con el mismo usuario por teléfono, u otra vía de comunicación, para corroborar la legitimidad de la solicitud.
- **No habilitar las macros de los documentos ofimáticos descargados** incluso si el propio fichero así lo solicita.
- **No hacer clic en ningún enlace** que solicite **datos personales ni bancarios.**
- En el caso de utilizar la **versión web para acceder al correo electrónico, no almacenar las credenciales** en el propio navegador. Antes de cerrar la sesión del navegador se debe asegurar cerrar la sesión de la cuenta de correo electrónico.

Buenas prácticas: Difusión

Boletín semanal interno UIB

Bones pràctiques: navegació web

- És important tenir actualitzats el navegador i els connectors instal·lats (només des de llocs oficials). Et recomanam que configuris els navegadors perquè s'actualitzin automàticament, bé de manera transparent a l'usuari o mitjançant notificacions que hauran de ser aprovades.
- Deshabilita o elimina les extensions en desús.

Bones pràctiques: xarxes socials

- Revisa la informació publicada. Tingues present que tot el que puges una xarxa social és permanent, encara que n'eliminis el compte.
- És important no basar-se en la configuració per defecte que proporcionen les plataformes.

CAMPAÑA

La Autenticación de Múltiples Factores (MFA)

Campaña MFA

https://seguretat.uib.es/concienciacion/campanas/mfa-es/ 90% Buscar

ESPAÑOL | CATALÀ

Reportar incidente: FORMULARIO 971 17 33 98

Universitat de les Illes Balears | SEGURETAT Tecnologies de la Informació

Actualidad Normativa Procedimientos Concienciación Avisos Buscar

Autenticación de Múltiples Factores (MFA)

CONTENIDOS

- Recomendaciones de uso de autenticación de múltiples factores
- Infografía: ¿Qué es la autenticación demúltiples factores (MFA)?
- Videos: ¿Cómo puedo configurar MFA en la UIB?
- Videos: Inicio de sesión con MFA
- Política de implantación de MFA
- Preguntas frecuentes

Campaña MFA

Videos: ¿Cómo puedo configurar MFA en la UIB?

Aplicación de autenticación (Configuración recomendada)

Microsoft Authenticator

Google Authenticator

Teléfono

SMS

Llamada

Videos: Inicio de sesión con MFA

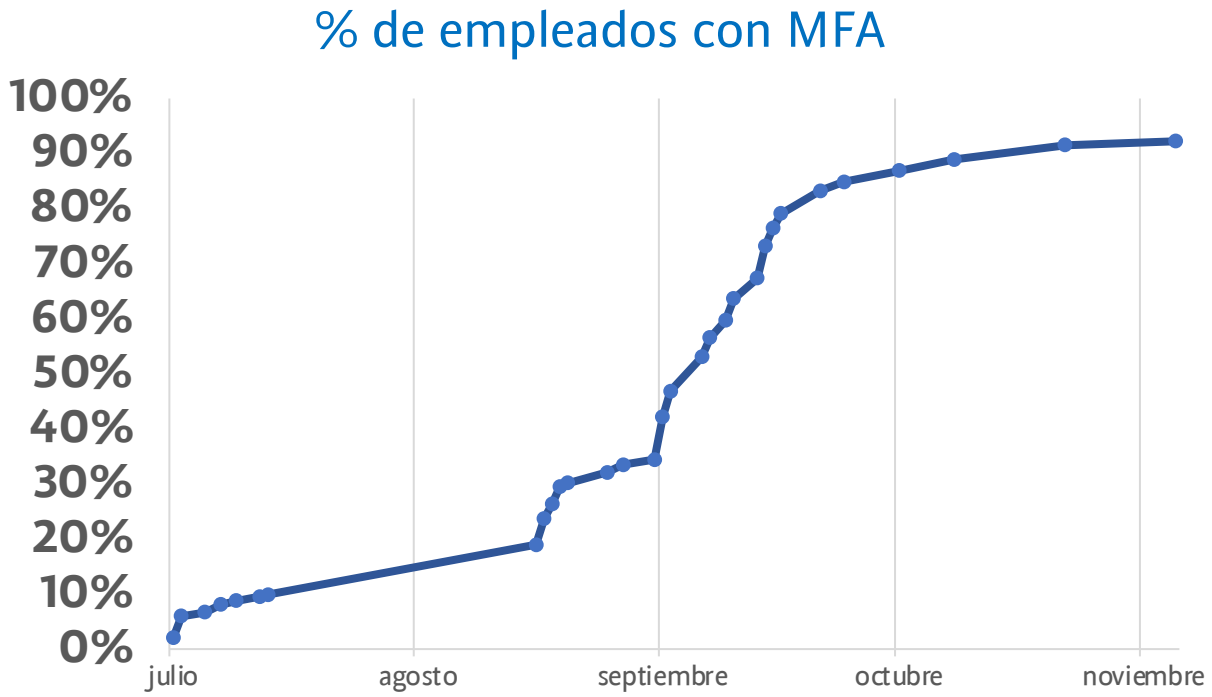
Teléfono de oficina

Llamada

Microsoft Authenticator

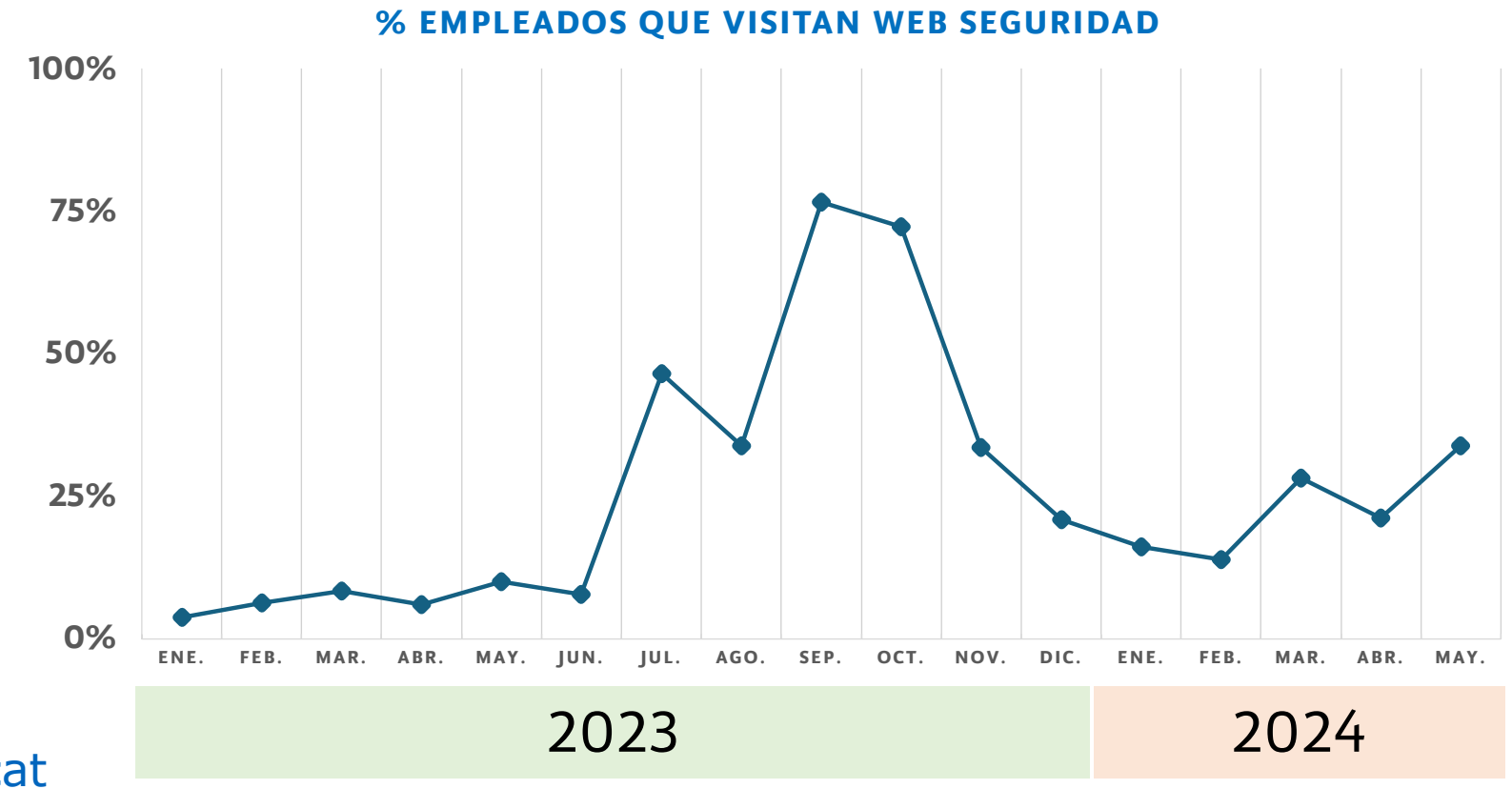
Google Authenticator

Campaña MFA



2023

Campaña MFA


% EMPLEADOS QUE VISITAN WEB SEGURIDAD
100%
75%
50%
25%
0%
ENE.
FEB.
MAR.
ABR.
MAY.
JUN.
JUL.
AGO.
SEP.
OCT.
NOV.
DIC.
ENE.
FEB.
MAR.
ABR.
MAY.
2023
2024

Colaboración con otras AAPP

Consell de Mallorca

Compartición del material creado con el Consejo de Mallorca

Difunde entre sus trabajadores los ciberconsejos y las buenas prácticas en el uso de las tecnologías de la información y la comunicación que ha elaborado la Universidad de las Islas Baleares (UIB).

Fuente: Diario de la UIB

Conclusiones

- Las acciones de concienciación que hemos realizado persiguen **fortalecer la seguridad TI de la UIB**.
- Aumento del nivel de **conocimiento y comprensión** sobre los **riesgos cibernéticos** (amenazas como phishing y malware).
- **Mejora en las prácticas** de seguridad:
  - Uso de MFA, creación de contraseñas seguras
  - El personal reporta actividades sospechosas, identificación de correos maliciosos
- **Mayor coordinación e intercambio de información** sobre buenas prácticas y amenazas potenciales.

"La concienciación en **ciberseguridad** es esencial para proteger no solo nuestros datos, sino también nuestra libertad y privacidad en el mundo digital."

- Bruce Schneier -


UIB
Universitat
de les Illes Balears