# Buenas Prácticas de IT

## CIBERSEGURIDAD

ie UNIVERSITY

# Software

**MANTÉN EL SOFTWARE Y EL ANTIVIRUS ACTUALIZADO SIEMPRE**

Comprueba que estás utilizando la última versión de todas las aplicaciones y antivirus de tus dispositivos. Para ello, accede a "Windows Update".

**UTILIZA MICROSOFT ONEDRIVE**

En caso de pérdida o robo, esto ayuda a minimizar la pérdida y fuga de datos.

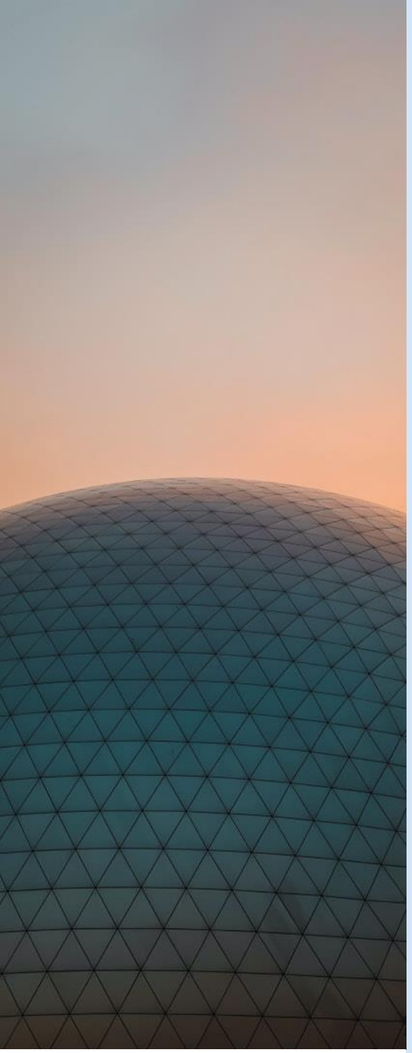
**SIGUE LAS RECOMENDACIONES CUANDO UTILICES APLICACIONES DE VIDEOCONFERENCIAS Y REUNIONES**

como Zoom, Microsoft Teams, para evitar accesos no deseados.

**NO DESCARGUES APLICACIONES QUE NO ESTÉN AUTORIZADAS POR IT.**

Pueden comprometer la seguridad de tu dispositivo y la información confidencial de IE.

ie UNIVERSITY



# Hardware

**EVITA COMPARTIR TU ORDENADOR.**
No prestes tu ordenador ni lo dejes desatendido.

**APAGA TU ORDENADOR TODOS LOS DÍAS.**
Cuando no lo utilices, tanto en la oficina como en casa cuando estés teletrabajando. No lo dejes bloqueado durante la noche o los fines de semana.

**TEN CUIDADO CON LOS PENDRIVES EXTRAÑOS.**
Primero compruébalos con el antivirus (Cortex).

**CONFIGURA UNA CONTRASEÑA SEGURA EN TUS DISPOSITIVOS MÓVILES.**
No uses las mismas en todas las aplicaciones y sitios.

ie UNIVERSITY

# Conectividad

**USA EL VPN PROPORCIONADO POR IE.**
Mantén una conexión segura a través del software VPN, Forticlient, con este perfil definido: IE_Staff_Split: uso general.
Ten en cuenta que las redes inalámbricas pueden ser objeto de abuso por parte de agentes malintencionados.

**EVITA ACCEDER EN ESPACIOS PÚBLICOS SIN VPN.** Existen programas que facilitan la interferencia de las plataformas y almacenan las pulsaciones del teclado.

**MANTENTE A SALVO USANDO TUS DATOS MÓVILES O REDES SEGURAS Y DE CONFIANZA.**

**TEN CUIDADO CON LAS REDES WIFI PÚBLICAS.**
Las redes WiFi públicas, como las de los hoteles, restaurantes y otros lugares públicos, no siempre son seguras. Lee atentamente las condiciones del proveedor y limita tus visitas a los sitios y el intercambio de tus datos en la medida de lo posible.
Nunca realices pagos ni accedas a tu cuenta bancaria.

ie UNIVERSITY

# Correo electrónico

## CUIDADO CON LOS CORREOS SOSPECHOSOS EN EL MÓVIL

Cuidado al leer los mails en los móviles, que no se muestran en su totalidad. Verifica el remitente, el asunto y la autenticidad.

## CUIDADO CON EL FRAUDE DEL CEO

Si recibes un correo pidiendo datos personales o financieros, verifica su autenticidad por otros medios. Recuerda que ni los bancos ni nosotros te pediremos por correo tus credenciales o trataremos la falta de espacio o los correos electrónicos retenidos.

## EVITA ACCEDER A SITIOS FALSOS

Antes de hacer clic en los enlaces abreviados (por ej., *bit.ly, goo.gl, ow.ly*), comprueba la fuente que te envió el enlace.

## CÓMO RECONOCER UN CORREO DE PHISHING

- Correos electrónicos no personalizados: “Estimado Cliente”.
- Ofertas tentadoras: “Una oferta que no puedes rechazar”.
- Te piden actuar de inmediato: a los phishers les encanta jugar con la urgencia.
- Sobre enlaces acortados, comprueba si son maliciosos ocultos pasando el cursor encima.
- Archivos adjuntos: si no proceden de alguien de confianza, aléjate de ellos. Los estafadores pueden incluso ocultar malware en archivos como los PDF.
- Enlaces con errores deliberados, tipográficos u ortográficos. Pueden ser URLs falsificadas.
- Mensajes mal redactados: con errores ortográficos y gramaticales.
- Solicitudes de información personal: Si te piden por correo datos personales, es probable que se trate de una estafa. Si para ello te piden que accedas a una URL, comprueba que ésta comience con “https” en lugar de “http”. La “s” significa “seguro”.

ie UNIVERSITY

# Correo electrónico

## Phishing

Es un delito cibernético en el que uno o más objetivos son contactados por correo electrónico o mensaje de texto por alguien que se hace pasar por una institución legítima para obtener datos confidenciales como detalles bancarios y contraseñas

Puedes informar de este tipo de correos a Microsoft para que lo analice a través del complemento de Outlook denominado “Informar de mensaje".

# Redes sociales

## PIENSA ANTES DE COMPARTIR

A todos nos gusta compartir fotos... Esto estará bien siempre y cuando no compartas muchos más detalles en tu perfil público, ya que podría ser una pista para que los criminales traten de suplantarte o algo peor.

## REVISA TU CONFIGURACIÓN DE PRIVACIDAD

Elimina la opción de geolocalización para tus publicaciones en las redes sociales, y configura tus dispositivos para que las fotos no contengan esta información.

Revisa tu configuración de privacidad y tus contactos en redes sociales.

Si no quieres que tus fotos se suban o te etiqueten, ¡avisa a tus amigos!

ie UNIVERSITY

# Contraseña

## SÉ ORIGINAL Y CREATIVO

**No utilices información personal:** fechas, lugares o cualquier dato que pueda ser investigado.

**No uses tu nombre de usuario.**

**No uses palabras ni grupos de palabras comunes.**

**No uses la misma contraseña para dos o más sitios.**

## LAS 10 PEORES CONTRASEÑAS

“123456”, “123456789”, “qwerty”, “password”, “1234567”, “12345678”, “12345”, “iloveyou”, “111111”, “123123”.

## CÁMBIALA PERIÓDICAMENTE

**Actualiza con frecuencia las claves.**

## MANTENLA EN SECRETO

**No compartas las contraseñas.** Trata de no escribirlas en ninguna parte.

**Procura evitar el uso de la opción *"recordar contraseña"*** de los navegadores.

ie UNIVERSITY

# Contraseña

**QUE SEA DIFÍCIL DE ADIVINAR...**

**Por su longitud:** incluye al menos 12 caracteres.

**Por su aleatoriedad:** combina números, símbolos, letras mayúsculas y minúsculas.

**...Y FÁCIL DE RECORDAR**

**Elige la primera letra de las palabras de una frase fácil de recordar** (refranes, canciones, citas, o incluso, alguna costumbre personal): “Café corto de café servido en vaso largo”: "CcDcSeVl".

**Cambia vocales por números:** " CcDcS3Vl".

**Personaliza las claves basadas en un mismo patrón:** "HelpMe0biWanKen0b1@FB" (Facebook), o "HelpMe0biWanKen0b1@AMZ" (Amazon).

ie UNIVERSITY

En definitiva, aplica el sentido común y recuerda que en Internet el mejor sistema de seguridad ¡eres tú!

ie UNIVERSITY

# ¡Gracias!