TU AYUDA PARA DIGITALIZARTE

cosmomedia.
marketing digital para tu negocio

# Semana de la Ciberseguridad

www.cosmomedia.es

contacto@cosmomedia.es

cosmomedia.
marketing digital para tu negocio

# DÍA 1.
# SEMANA DE LA CIBERSEGURIDAD

Cerca de tres millones de pymes se encuentran desprotegidas frente a los ciberataques
El primer paso para protegernos es saber a qué nos enfrentamos.

## PHISING Y RAMSONWARE, LOS ATAQUES MÁS FRECUENTES

**Phising:** Es una técnica de hackeo consistente en suplantar la identidad de una persona o empresa para acceder a información confidencial de sus posibles víctimas, tales como clientes, proveedores o empleados.

**Ramsonware:** Los hackers secuestran el sistema y los datos, cifrando el contenido y pidiendo un rescate a cambio de descifrarlo. Este rescate suele ser mediante sistemas de pago virtuales que permiten el anonimato (Bitcoins)

## ¿CÓMO PUEDO PROTEGERME?

No abrir correos de usuarios desconocidos

Revisar los enlaces antes de hacer clic
Hay que desconfiar en los enlaces acortados.

Desconfiar de los ficheros adjuntos

Cuidado con el SPAM
Nunca facilites tu informacion mediante correo electronico

Control de dispositivos extraíbles, usar únicamente
CD,DVD, USB,MOVILES...
Proporcionados por la empresa o revisados por el administrador previamente en busca de malware

No usar el WIFI
En dispositivos ajenos a la empresa, es un foco de infección muy alto.

Tener siempre actualizado
El sistema operativo y el software del dispositivo

Utilizar contraseñas robustas

Usar aplicaciones oficiales

Navegar por webs seguras

## Y NO OLVIDES REALIZAR COPIAS DE SEGURIDAD PERIÓDICAS E INTENTAR TRABAJAR SIEMPRE EN LA RED DE LA EMPRESA O EN LA NUBE

cosmomedia.
marketing digital para tu negocio

# DÍA 2.
# SEMANA DE LA CIBERSEGURIDAD

El 43% de los ataques se efectúan contra pequeñas y medianas empresas. El primer paso para protegernos es saber a qué nos enfrentarnos

## CONOCIENDO RAMSONWARE

Este tipo de Malware está relacionado con los avances en la criptografía y permite una alta rentabilidad económica a los ciberdelincuentes por la gran facilidad para ocultarse, ya que los pagos suelen pedirse en forma de criptomonedas (Bitcoins)

Bitcoin es una moneda virtual y no existe una autoridad o ente de control que sea responsable de su emisión o registro de movimientos.

## TIPOS DE RAMSOMWARE

**Hoax** Simula el cifrado de nuestro equipo y nos exigen un pago por recuperar nuestros archivos

Utiliza un señuelo, como un falso software o soporte. Suele ser un anuncio emergente molesto que nos ofrece una solución rápida a nuestro problema.

**Scareware**

**Bloqueadores de pantalla**

Impiden el uso de nuestro ordenador mediante una ventana que ocupa toda nuestra pantalla y no puede ser cerrada. El mensaje que aparece puede ser:

Un mensaje de las fuerzas de seguridad indicando que han detectado actividades ilegales solicitando el pago de una multa

Simula el cifrado de nuestro equipo y nos exigen un pago por recuperar nuestros archivos

**Doxware** Amenaza al usuario con hacer públicos los datos personales extraídos

**De cifrado**

Es el mas peligroso. Cifran nuestros datos y exigen un rescate (hay una variante mas peligrosa llamada Wiper, que no cifra sino borra directamente los archivos haciendo imposible su recuperación)

**EVITA ABRIR Y/O DESCARGAR ARCHIVOS SOSPECHOSOS DE REMITENTES DESCONOCIDOS O CON FORMATOS EJECUTABLES (.EXE...)**

cosmomedia.
marketing digital para tu negocio

# DÍA 3.
# CIBERSEGURIDAD Y TELETRABAJO

El teletrabajo ha venido para quedarse.
Pero esto también crea nuevos riesgos de seguridad

## PROTEGERNOS EN CASA

El desconocimiento hace que muchos trabajadores usen portátiles o teléfonos inteligentes personales que no ofrecen el necesario cifrado de datos de alta calidad. Esto se convierte en un agujero importante de seguridad que los ciberdelincuente suelen aprovechar.

## ERRORES FRECUENTES

### Contraseñas 123456

O similares, las contraseñas deben ser robustas y modificadas cada 6 meses.

### Los equipos deben estar actualizados

cualquier software desactualizado significa que es susceptible de tener fallos en la seguridad y vulnerabilidades

### Lo gratis puede salir caro,debemos usar siempre programas originales y de confianza

### No usar la nube o red de la empresa

En caso de desastre, la recuperación de datos es posible si tenemos nuestros datos en sitios donde se realizan periódicamente copias de seguridad.

### No tener un firewall

Es imprescindible en la estrategia de seguridad de una empresa. Este "portero" de nuestra red, impedirá que las amenazas externas accedan a nuestro sistema

### Debemos conectarnos por VPN Redes Privadas Virtuales

Comúnmente conocidas por sus siglas en inglés VPN. Este acceso a través de Internet de forma segura permite la movilidad del trabajador y mantiene seguros todos nuestros datos.

### No olvides realizar copias de seguridad periodicas

No debemos dejar nuestros datos en lugares donde no se realizan copias. Siempre debemos dejar nuestros datos en los espacios donde la empresa hace backup. Si no lo sabes, pregúntalo. No te arriesgues a perder tus datos.

**PARA PROTEGERNOS EN CASA USA CONEXIÓN VPN, PROGRAMAS ACTUALIZADOS Y SIEMPRE GUARDA EN EL ESPACIO QUE REALICE BACKUP.**

cosmomedia.
marketing digital para tu negocio

# DÍA 4.
# CIBERSEGURIDAD Y TELETRABAJO

El coste medio al que tiene que hacer frente una pyme en caso de un ataque es de 35.000 euros, por lo que el 60% de las empresas atacadas termina por cerrar el negocio.

## PLAN DE RESPUESTA ANTE INCIDENTES

Una acción de carácter preventivo es la de contar con un plan de actuación o respuesta ante incidentes.

## FASES DEL PLAN

### Preparacion

- Asignar quien debe realizar la gestión
- Definir donde está la documentación necesaria para abordar el plan
- Tener a mano con quien debemos contactar en caso de incidencia

### Detención y análisis

Se ha de clasificar el incidente para determinar cómo abordarlo

### Contención, resolución y recuperación

Se han de seguir los pasos para recuperar la actividad

### Una vez cerrado el incidente

Debemos registrar todo lo sucedido y elaborar la documentación necesaria para futuros problemas

## ¿QUÉ HACER SI ME AFECTA?

- NO pagar nunca el rescate, porque no garantiza recuperar la información
  Si pagas puedes ser objeto de posteriores ataques.
- Aplicar el plan de respuesta ante incidentes
- Utilizar las copias de seguridad realizadas

**NO PAGUES EL RESCATE, ELABORA UN PLAN PARA ESTE TIPO DE PROBLEMAS, DOCUMÉNTALO TODO Y UTILIZA LAS COPIAS DE SEGURIDAD.**

cosmomedia.
marketing digital para tu negocio

# DÍA 5. RESPUESTA FRENTE A UN CIBERATAQUE


Solo el 36% de las pymes dispone de los protocolos básicos de seguridad.

Cerca de tres millones de pymes se encuentran desprotegidas frente a los ciberataques.

## ¿QUÉ HACER SI ME HAN HACKEADO?

Aun teniendo todas las precauciones, siempre podemos ser victimas de un ataque.
Si nos encontramos en esta situacion.... que no cunda el pánico:

## PLAN DE RESPUESTA

- Aísla el equipo de la red, para evitar que se propague

---

- Cambia inmediatamente todas las contraseñas

---

- Clonar el disco duro Puede que ahora no exista solución al problema, pero es posible que en un futuro si la haya. Es recomendable desinfectarlo antes de guardarlo con herramientas de antivirus y antimalware

---

- Denunciar el incidente

(Delitos telemáticos) y Policía Nacional (Brigada de Investigación Tecnológica)

---

- Recuperar y restaurar el equipo

Para ello, usaremos las copias de seguridad.

## Y RECUERDA...

- NO pagar nunca el rescate, ya que no garantiza recuperar la información y si pagas, puedes ser objeto de futuros ataques.
- Aplicar el plan de respuesta ante incidentes.
- Utilizar las copias de seguridad realizadas.

**DESCONECTA EL CABLE DE INTERNET Y AISLA EL EQUIPO INFECTADO, APAGANDO CUALQUIER CONEXIÓN CON OTROS EQUIPOS Y SISTEMAS.**

cosmomedia.

marketing digital para tu negocio

# Semana de la Ciberseguridad

Tu especialista en digitalización aplicada a la pyme

www.cosmomedia.es

contacto@cosmomedia.es