

MAPFRE IMPULSA UNA #CULTURACIBERSEGURA PARA PREVENIR LOS CIBERRIESGOS



La pandemia ha acelerado la interconexión digital de personas y empresas, creando un entorno propicio para el incremento de los ciberataques. Por eso, MAPFRE ha lanzado una campaña interna de concienciación en ciberseguridad para mejorar la prevención y sensibilización frente a este tipo de riesgos.



VISITA LA EDICIÓN DIGITAL DE LA REVISTA
EN WWW.ELMUNDODEMAPPFRE.COM



TEXTO **PABLO FUENTES** | IMÁGENES **MAPPFRE**

La ciberseguridad es un eje fundamental de la transformación digital, ya que en el entorno de las nuevas tecnologías y la era digital cada vez estamos más expuestos a la ciberdelincuencia. Esta situación se ha visto agravada por la pandemia de la covid-19, que ha acelerado la digitalización y la conectividad de personas y empresas, creando así un entorno propicio para los ciberataques, como el que MAPFRE afrontó con éxito en 2020 en España, uno de los momentos más complejos en la historia de la compañía.

En su informe *Ciberamenazas y tendencias. Edición 2021*, el CCN-CERT (Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia) habla de un incremento en el número de incidentes y en su peligrosidad, debido a la digitalización forzosa en la que la sociedad se ve envuelta.

Por poner una cifra, el Instituto Nacional de Ciberseguridad de España (INCIBE) gestionó 133.155 incidentes durante el año 2020, de los que el 80 % hicieron referencia tanto a ciudadanos como empresas. Estos datos duplican la cifra del año anterior, por lo que los expertos comenzaron a hablar de una ciberpandemia.

En este contexto, ahora cobra protagonismo el concepto de responsabilidad individual. Es decir, cualquiera de nuestras acciones puede convertirse en una gran amenaza para nuestra seguridad. De hecho, el 95 % de los ataques o incidentes en materia de ciberseguridad se debe a fallos humanos, según

THE FIREWALL MINDSET ES UNA CAMPAÑA 100 POR 100 DIGITAL CUYO OBJETIVO ES ENSEÑAR A LOS USUARIOS A PREVENIR Y ACTUAR ANTE LOS ATAQUES MÁS RECURRENTES

el estudio Cyber Security Intelligence Index de IBM, por lo que la prevención a través de la concienciación de los empleados debe ser una prioridad en la agenda de todas las corporaciones.

Por esta razón, MAPFRE ha lanzado una campaña de concienciación en ciberseguridad, denominada Firewall Mindset MAPFRE, #CulturaCibersegura, que busca impulsar la cultura de seguridad de MAPFRE, en el marco del Plan de Ciber Resiliencia (PCR).

Además, la iniciativa forma parte del escenario de Protección de la información de Digital Workplace, un proyecto que ofrece a los profesionales de la compañía, a través de herramientas de colaboración digital, la oportunidad de trabajar de una forma más ágil, colaborativa y segura.

Se trata de una campaña 100 por 100 digital cuyo objetivo es enseñar a los usuarios a

prevenir y actuar ante los ataques más recurrentes. A través del *storytelling* y una metodología basada en la gamificación, muy divertida y amena, los ciberagentes aprenden con casos reales y entrenan sus habilidades OPDA (Observa, Piensa, Decide y Actúa), el mantra del proyecto, que es lo que nos permitirá estar preparados ante los próximos ciberataques.

MAPFRE quiere que todos sus profesionales sean conscientes de la importancia que tiene nuestro comportamiento seguro en Internet en el entorno profesional, y también en nuestro ámbito personal y familiar. Además, es una estupenda oportunidad para aumentar y reforzar los conocimientos en materia de ciberseguridad.

A través de la gamificación, los usuarios resuelven casos reales en distintas modalidades de ciberataque.

MAPFRE incorpora a sus primeros 7.300 ciberagentes

La campaña comenzó a finales de 2021 en España y ya han participado más de 7.300 personas, de las cuales 3.800 ya han recibido su diploma como ciberagentes de la compañía. Todos ellos han pasado por distintas pruebas, que van desde la visualización de un webisodio, el informe de una experta con la explicación del caso, unos tips o

POR PONER UNA CIFRA,
EL INSTITUTO NACIONAL DE
CIBERSEGURIDAD DE ESPAÑA
(INCIBE) GESTIONÓ

133.155

INCIDENTES DURANTE EL AÑO
2020, DE LOS QUE EL
80 %

HICIERON REFERENCIA
TANTO A CIUDADANOS COMO
EMPRESAS. ESTOS DATOS
DUPLICAN LA CIFRA DEL AÑO
ANTERIOR, POR LO QUE LOS
EXPERTOS COMENZARON
A HABLAR DE UNA
CIBERPANDEMIA.

claves de este, un examen o caso abierto y finalmente la solución y el cierre del caso. En total, en la plataforma se alcanzaron más de 159.594 visualizaciones de vídeo, cerca de 1.781 likes y 2.013 comentarios

En 2022 se está completando el despliegue de la campaña en España y **se está iniciando el lanzamiento** en el resto de las regiones y países de MAPFRE.

Esta campaña es una de las iniciativas desarrolladas por el Grupo de Trabajo de Concienciación en Ciberseguridad de MAPFRE, integrado por la Dirección Corporativa de Seguridad, el Área Corporativa de Personas y Organización y el Área Corporativa de Relaciones Externas y Comunicación, desde el que se impulsan también otras acciones dirigidas a crear cultura de seguridad en la empresa.

Destacan, por ejemplo, el despliegue de cursos de formación en seguridad integral a 22.000 empleados y de privacidad de datos a 19.000; la distribución a más de 11.000 profesionales en España de una funda de protección para tarjetas de crédito; la publicación trimestral en la Intranet Global y la App Personas de vídeos e infografías con consejos sobre ciberseguridad; y la realización de simulaciones y ciberejercicios en distintos países, para medir a eficacia de las acciones de formación y concienciación. 

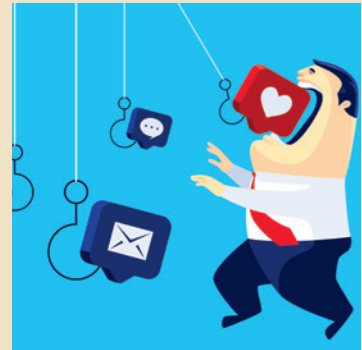
LOS TIPOS DE CIBERATAQUE QUE MÁS HAN AUMENTADO DURANTE LA PANDEMIA

Según el Instituto Nacional de Ciberseguridad de España (INCIBE), las modalidades de ciberataques que más auge tuvieron en 2020 fueron las siguientes:



PHISHING CORPORATIVO O BEC (BUSINESS EMAIL COMPROMISE)

aprovechando el incremento de la situación del teletrabajo. Dentro de este ataque, destaca el fraude del CEO, con un crecimiento del 15 %.



MALWARE A MEDIDA

haciendo uso del reclamo de la crisis sanitaria, los ciberdelincuentes lanzan campañas masivas de phishing. Además, han modificado el tipo de malware para lograr un impacto de ataque mayor.



RANSOMWARE

más dirigido y peligroso, que permite a los ciberdelincuentes aumentar el precio del rescate y aumentar sus beneficios.



CADENA DE SUMINISTROS

ha aparecido como novedad en las listas de tendencias de ciberataques, como consecuencia de la falta de madurez y eficacia en la seguridad de procesos de muchas organizaciones. Uno de los mayores incidentes que podemos destacar fue la vulneración del código fuente de la nube de Microsoft.