talento HACKER

EL DÍA A DÍA DEL HACKER ÉTICO

ANTE UN ATAQUE DE *RANSOMWARE*

Descubre cómo los distintos perfiles *hacker* ayudan a Adrián a defender y prevenir su empresa de ataques *ransomware*.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

EN UNA MAÑANA DE UN AMANECER CUALQUIERA...

DOCE PERSONAS RECIBEN UNA VIDEOLLAMADA.

RING! RING!

MIENTRAS TANTO EN LA EMPRESA DE ADRIÁN...

Escuchadme, os he llamado porque necesito vuestra ayuda.

Sí. Nosotros, el ciberequipo, te ayudaremos.

CIBEREQUIPO

Natalia

Jaime

Laura

Omar

Mirella

Marta

Ramón

Sandra

Antonio

Andrés

Carmen

Mateo

Estamos en apuros.

En todas las pantallas de la empresa aparece un mensaje pidiendo un rescate para recuperar la información. Pensamos que podría ser un...

A-A-AA!!

ALARM!

¡RANSOMWARE!

LAURA - DIRECTORA DE SEGURIDAD DE LA INFORMACIÓN

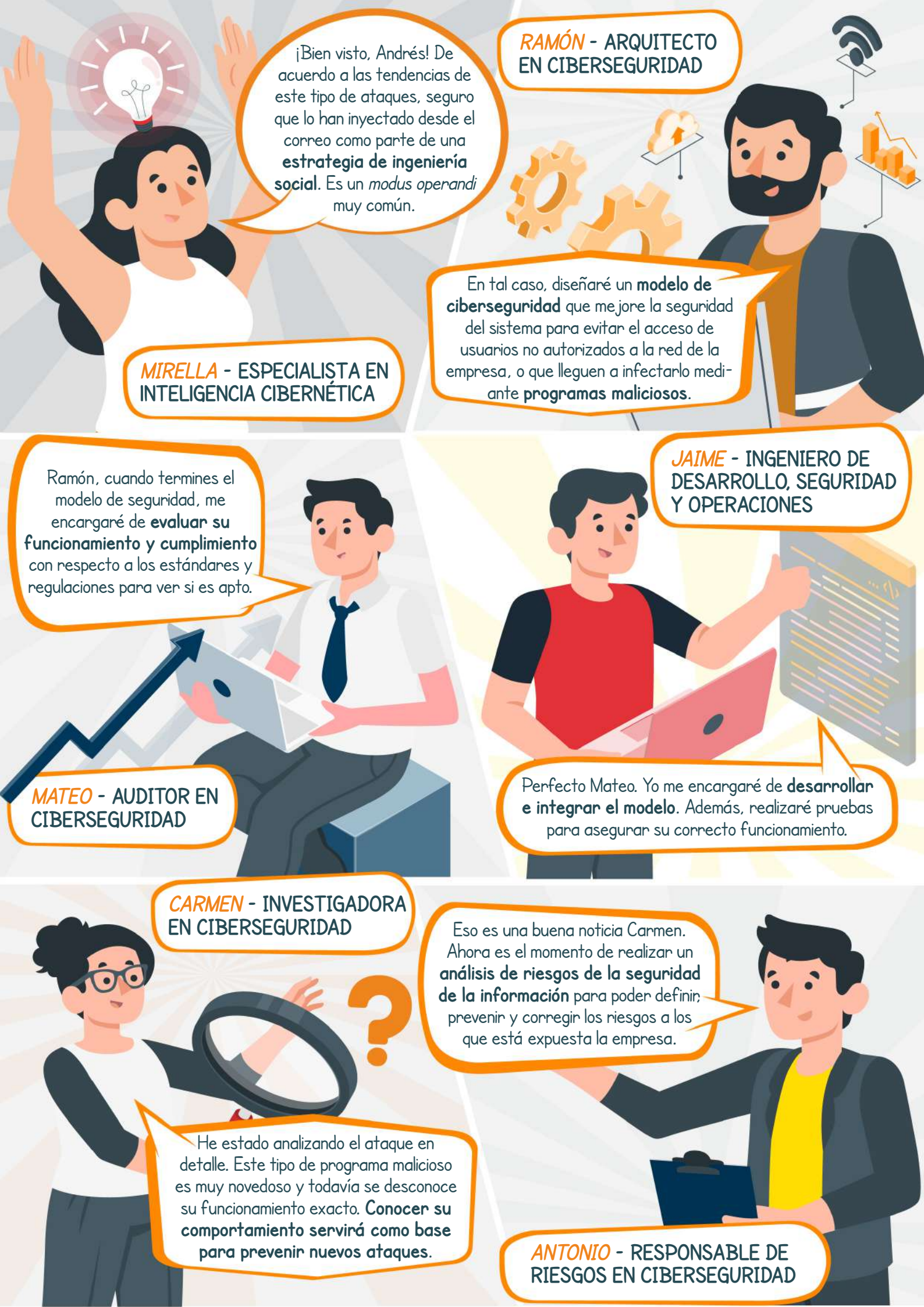
Sí, seguro que es un *ransomware*, pero no te preocupes, hemos establecido una **estrategia**, unas **políticas** y un **procedimiento** para este tipo de ataques. Mi equipo se pondrá de inmediato a ayudarte.

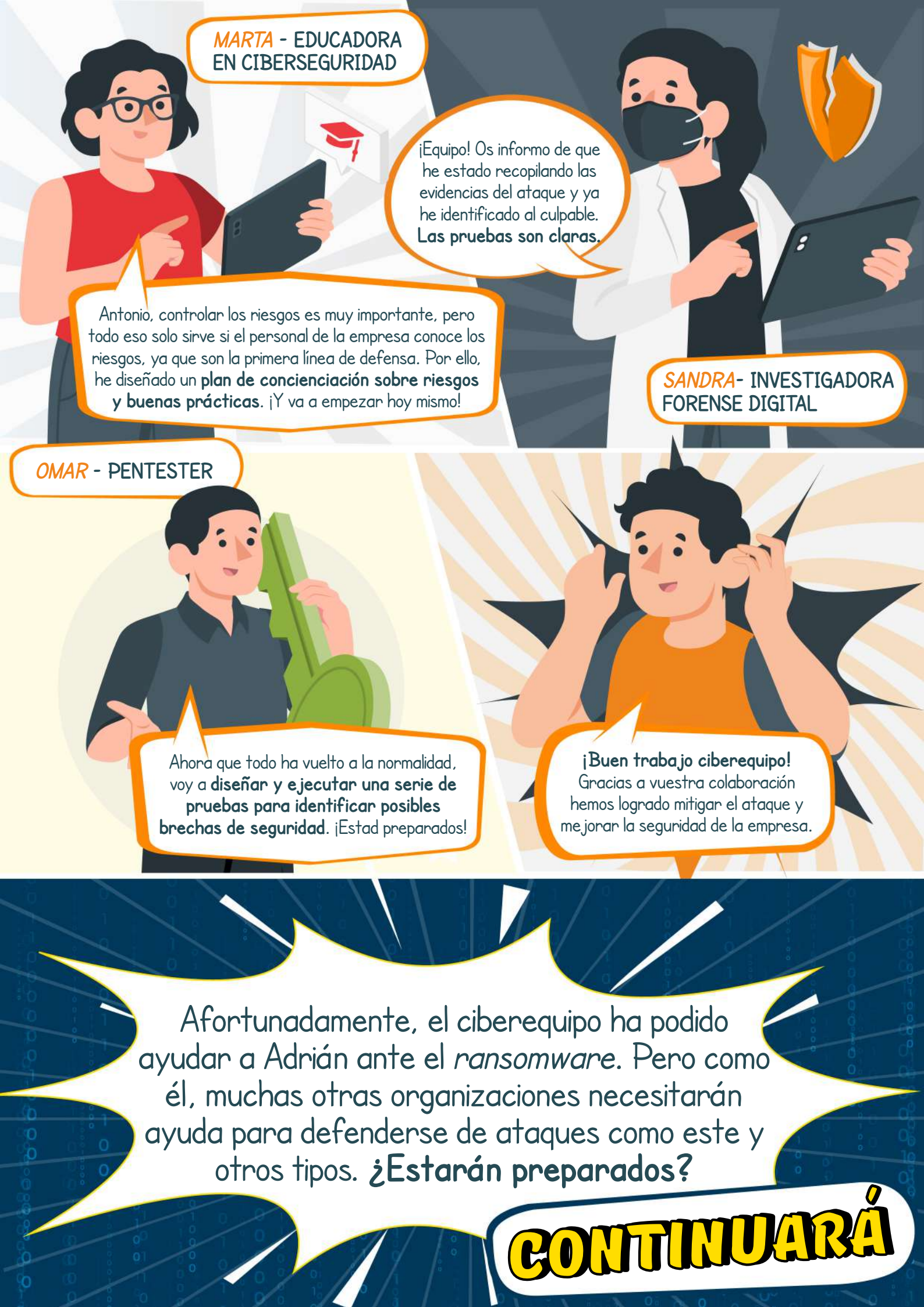
ANDRÉS - RESPONSABLE DE CUMPLIMIENTO CIBERNÉTICO

Antes de nada, debéis aislar los equipos infectados y debemos asegurarnos de que la privacidad de los datos no se ha visto comprometida e informar a las partes implicadas para cumplir con la **Ley de Protección de Datos Personales y Garantía de los Derechos Digitales**.

NATALIA - RESPONSABLE DE INCIDENTES CIBERNÉTICOS

Así es Andrés, ya he realizado un informe donde he analizado y evaluado el impacto de este incidente. Llamaré a Sandra, que es investigadora forense, para preservar y analizar las evidencias que recopilemos antes de restaurar la funcionalidad de los sistemas. Tenemos que recurrir a las **copias de seguridad** que son muy importantes para restablecer la actividad de la empresa. Además, monitorizaremos los sistemas para detectar posibles amenazas nuevas.


¡Bien visto, Andrés! De acuerdo a las tendencias de este tipo de ataques, seguro que lo han inyectado desde el correo como parte de una **estrategia de ingeniería social**. Es un *modus operandi* muy común.
MIRELLA - ESPECIALISTA EN INTELIGENCIA CIBERNÉTICA
RAMÓN - ARQUITECTO EN CIBERSEGURIDAD
En tal caso, diseñaré un **modelo de ciberseguridad** que mejore la seguridad del sistema para evitar el acceso de usuarios no autorizados a la red de la empresa, o que lleguen a infectarlo mediante **programas maliciosos**.
Ramón, cuando termines el modelo de seguridad, me encargaré de **evaluar su funcionamiento y cumplimiento** con respecto a los estándares y regulaciones para ver si es apto.
MATEO - AUDITOR EN CIBERSEGURIDAD
JAIME - INGENIERO DE DESARROLLO, SEGURIDAD Y OPERACIONES
Perfecto Mateo. Yo me encargaré de **desarrollar e integrar el modelo**. Además, realizaré pruebas para asegurar su correcto funcionamiento.
CARMEN - INVESTIGADORA EN CIBERSEGURIDAD
He estado analizando el ataque en detalle. Este tipo de programa malicioso es muy novedoso y todavía se desconoce su funcionamiento exacto. **Conocer su comportamiento servirá como base para prevenir nuevos ataques**.
Eso es una buena noticia Carmen. Ahora es el momento de realizar un **análisis de riesgos de la seguridad de la información** para poder definir, prevenir y corregir los riesgos a los que está expuesta la empresa.
ANTONIO - RESPONSABLE DE RIESGOS EN CIBERSEGURIDAD



Afortunadamente, el ciberequipo ha podido ayudar a Adrián ante el *ransomware*. Pero como él, muchas otras organizaciones necesitarán ayuda para defenderse de ataques como este y otros tipos. **¿Estarán preparados?**

CONTINUARÁ

EL DÍA A DÍA DEL HACKER ÉTICO

ANTE UN ATAQUE DE *RANSOMWARE*

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD