CIBERSEGURIDAD

EL IMPACTO EN LAS EMPRESAS Y CÓMO GESTIONAR EL RIESGO.

LIFE IS FOR SHARING.

T-SYSTEMS SUBSIDIARIA DE DEUTSCHE TELEKOM PARA LAS PRINCIPALES CORPORACIONES

T-Mobile

T-Mobile ofrece soluciones de telefonía celular en los Países Bajos, Austria, República checa y los Estados Unidos de América.

Telekom

Las subsidiarias de Telekom brindan productos y servicios para la red fija, comunicaciones móviles, IPTV, servicios en línea y en la nube.

T-Systems

T-Systems ofrece soluciones de TIC para las principales corporaciones y organizaciones del sector público que tienen presencia global y alianzas a través de los socios.

Datos y Cifras

€ 22.2 B	217,000	€ 74.9 B	169 M	50	1.6 M
EBITDA Ajustado	Empleados	Ingresos	Clientes Móviles	Países	Sistemas Gestionados

CONSTRUYENDO LA ERA DIGITAL

1.5K

Profesionales de Seguridad cibernética

5G

Integración de la seguridad de la red en la arquitectura de la red central.

>1.6K

Proyectos de soluciones digitales en el 2018

>20años

De experiencia en Seguridad cibernética

65K

Sistemas live cloud

95% DAX

y 19 de la Fortuna 100 compañías son nuestros clientes

4.8K

Expertos en digitalización en todo el mundo.

>600

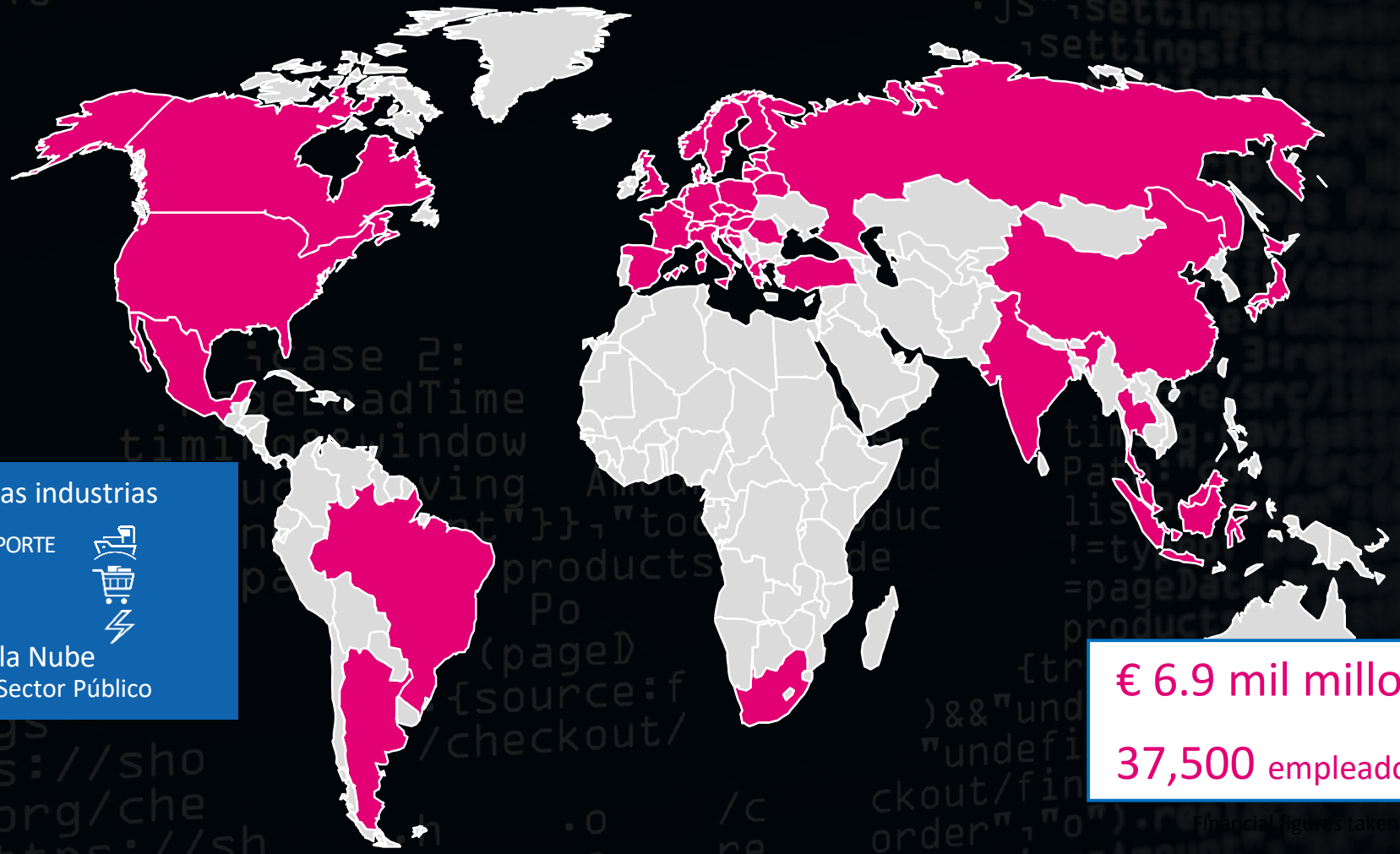
Los clientes empresariales de todo el mundo están a cargo de nosotros

Alta satisfacción de proyectos con:

98%

Calificación promedio de > 1,600 proyectos de soluciones digitales en 2018

UNIDADES DE NEGOCIO DE T-SYSTEMS



Servicios de TI y TC en todas las industrias

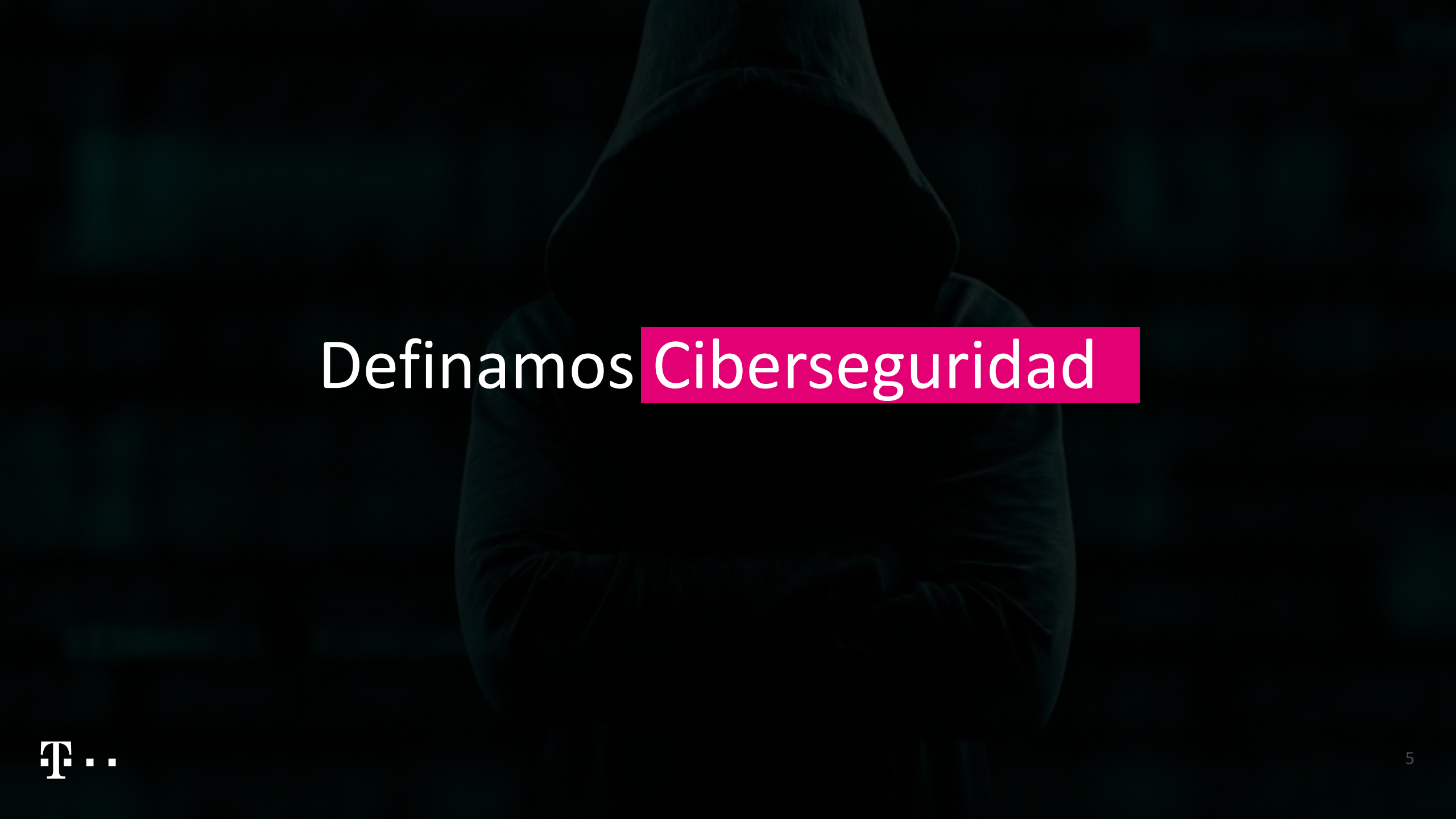
AUTO & MI
VIAJES Y TRANSPORTE
PÚBLICO
MINORISTAS
SALUD
ENERGÍA

Pioneros en computación en la Nube
Corporaciones Multinacionales & Sector Público

€ 6.9 mil millones Ingresos

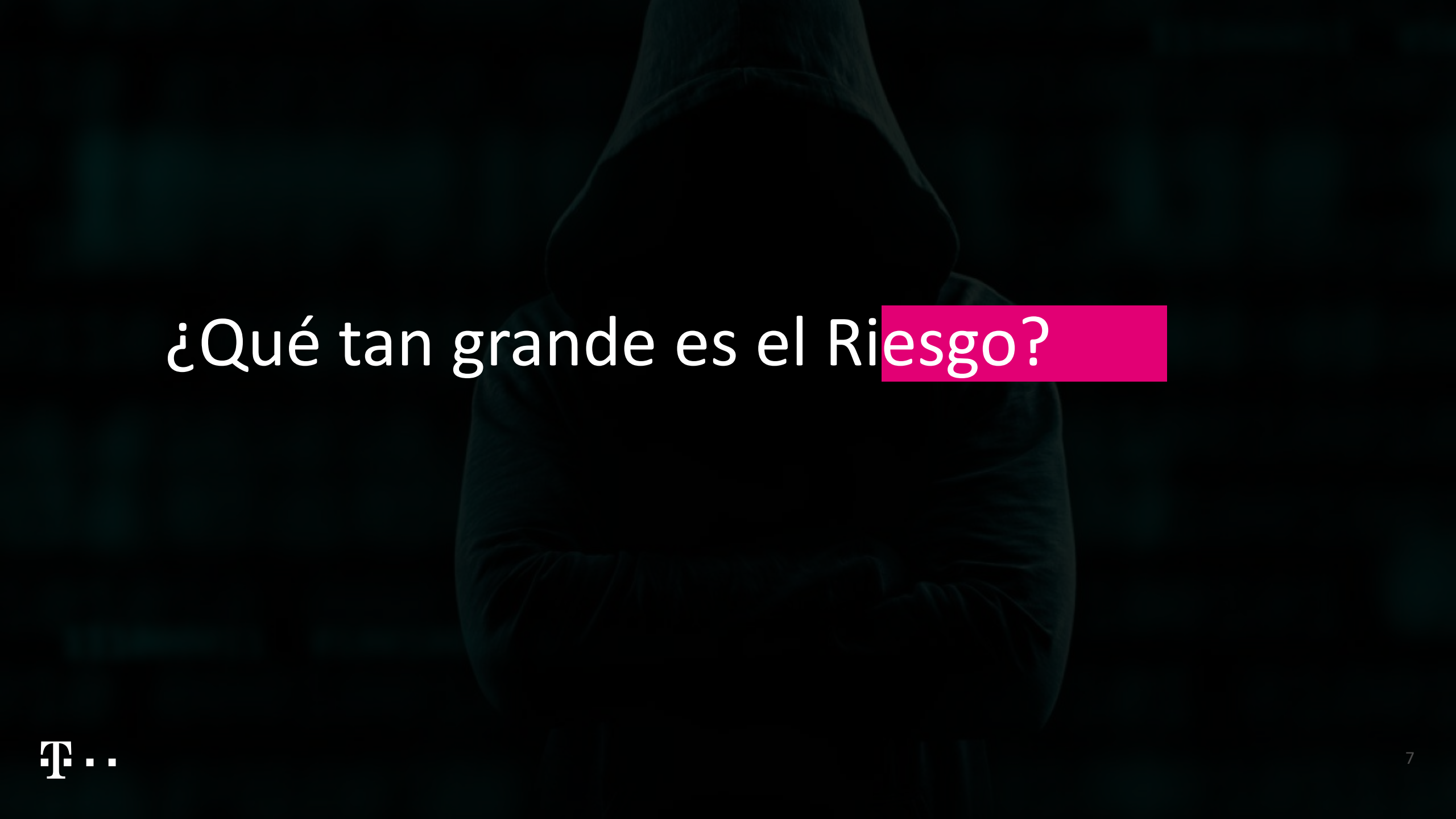
37,500 empleados

Financial figures taken from DT's 2018 annual report



Definamos Ciberseguridad

Ciberseguridad vs Seguridad de la información



¿Qué tan grande es el Riesgo?

CYBERATAQUES POR DÍA EN LA INFRAESTRUCTURA DE DEUTSCHE TELEKOM

PUNTO MÁXIMO:
48 MN.

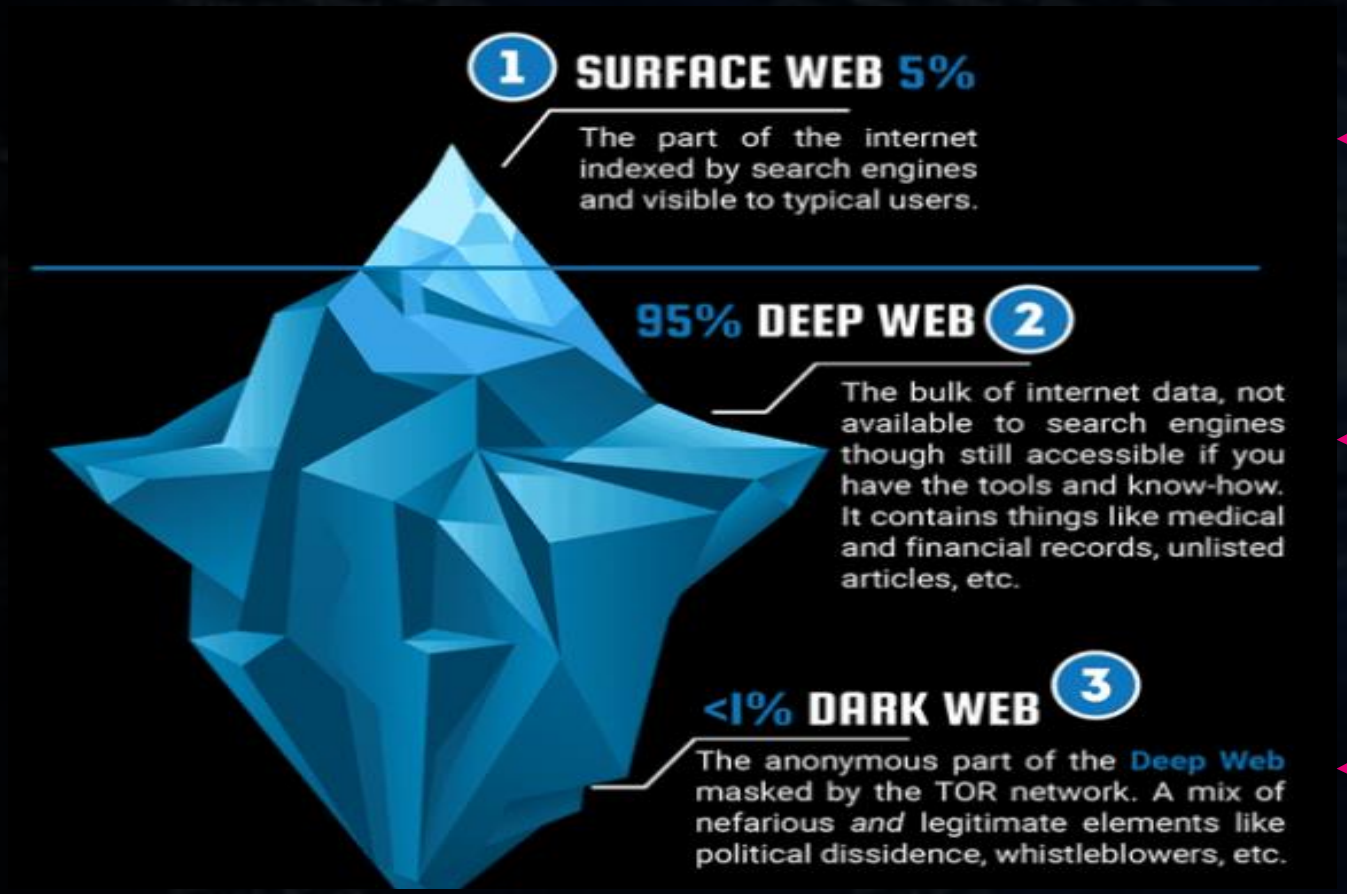
Ataques por día en Junio del 2020

Dispositivos conectados a Internet

- 2009: 3 mil millones
- 2020: 30 mil millones
- 4 dispositivos por cada habitante en el mundo

620 físicas y 3,400 instalaciones honeypot

QUE VISIBILIDAD TENEMOS DE LA INFORMACIÓN EN INTERNET?



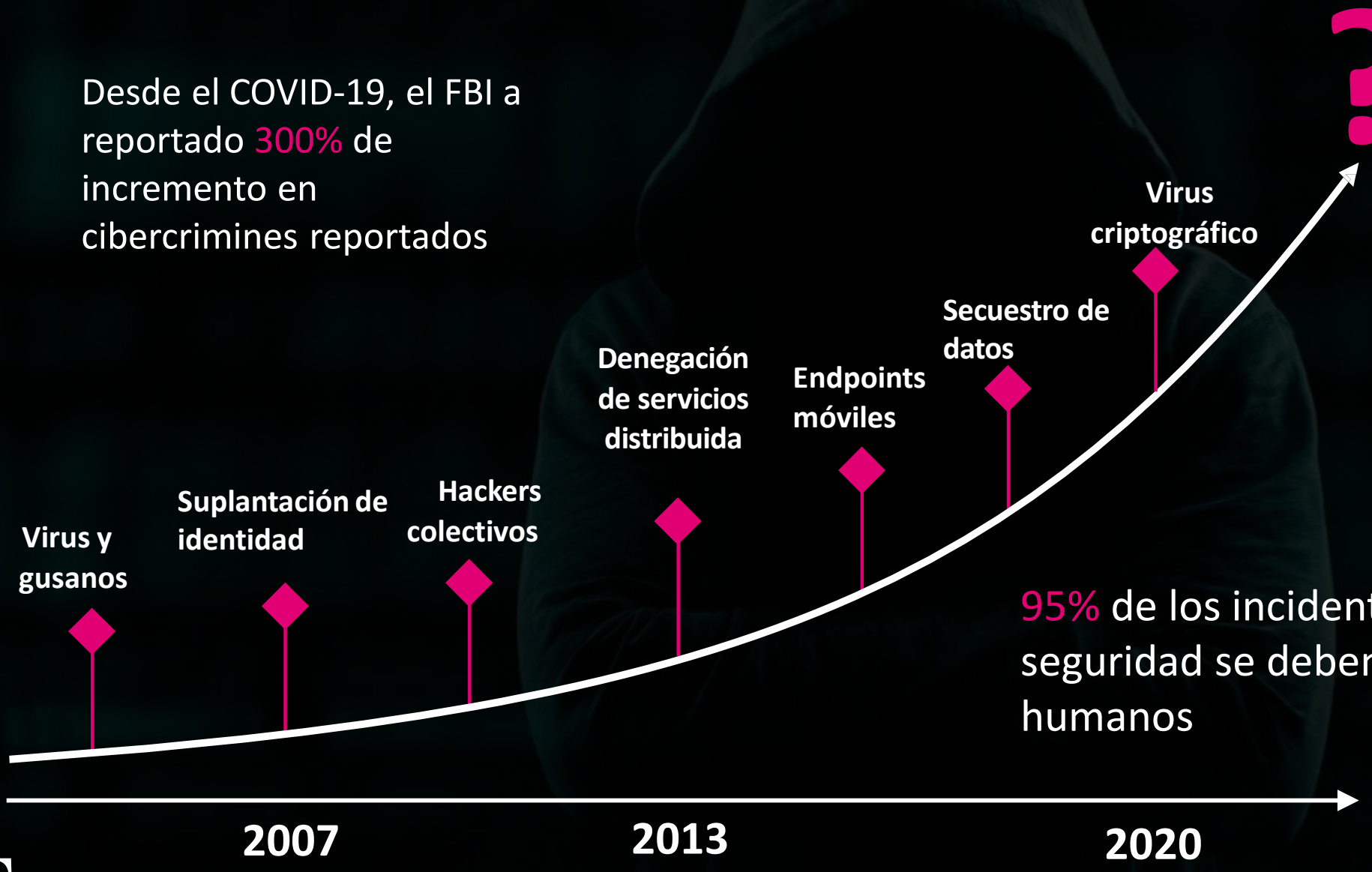
Navegación WEB

Deep WEB

Dark WEB

¡LOS ATAQUES SE VUELVEN CADA VEZ MAS SOFISTICADOS!

Desde el COVID-19, el FBI a reportado 300% de incremento en cibercrimines reportados



95% de los incidentes de seguridad se deben a errores humanos

ATAQUES A LA INFRAESTRUCTURA CRÍTICA

Nov 2016

900.000 Personas sin internet

Red de robot informáticos - Ataque al enrutador

Mayo 2017

Fallo del sistema nacional de salud

Secuestro de datos a hospitales de Inglaterra.

Junio 2018

Intrusión a través de la red de la oficina

Ciberataques al sector energético

Mayo 2019

Administración paralizada

Ataque a la red de la ciudad de Baltimore

Julio 2019

Cadena hospitalaria de California

Secuestro de datos provoca cierre permanente

FUENTES Y MOTIVOS DE LOS CIBERATAQUES

INTERNO

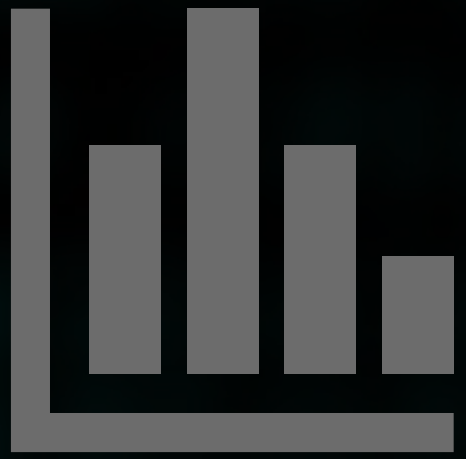
- Empleados de confianza que pierden información accidental.
- Empleados descontentos o ex empleados que intentan dañar su negocio.
- Empleados malintencionados con acceso legítimo a sistemas e información crítica.

EXTERNO

- Delincuentes organizados o grupo delictivos.
- Hackers profesionales ya sean maliciosos o no.
- Hackers aficionados o llamados “script kiddies”

OBJETIVOS

CUAL SERÍA EL MAYOR IMPACTO PARA SU NEGOCIO CAUSADO POR UN CIBERATAQUE?



VE A www.menti.com

Y USA EL CÓDIGO 50 36 704

Tiempo de votar

IMPACTO DE UN CIBERATAQUE

Costo económico

Los ataques cibernéticos a menudo resultan en pérdidas financieras sustanciales derivadas de:

- Pérdida de activos
- Robo de información corporativa
- Robo de información financiera(por ejemplo datos bancarios o de tarjetas de pago)
- Robo de dinero
- Pérdida de negocio o contrato
- Retrocesos operativos

Daño reputacional

Los ataques cibernéticos dañan la reputación de su empresa y la confianza que sus clientes tienen de usted provocando:

- Pérdida de clientes y contratos.
- Pérdida de ventas.
- Reducción de beneficios.
- Relaciones comerciales con socios de negocio.

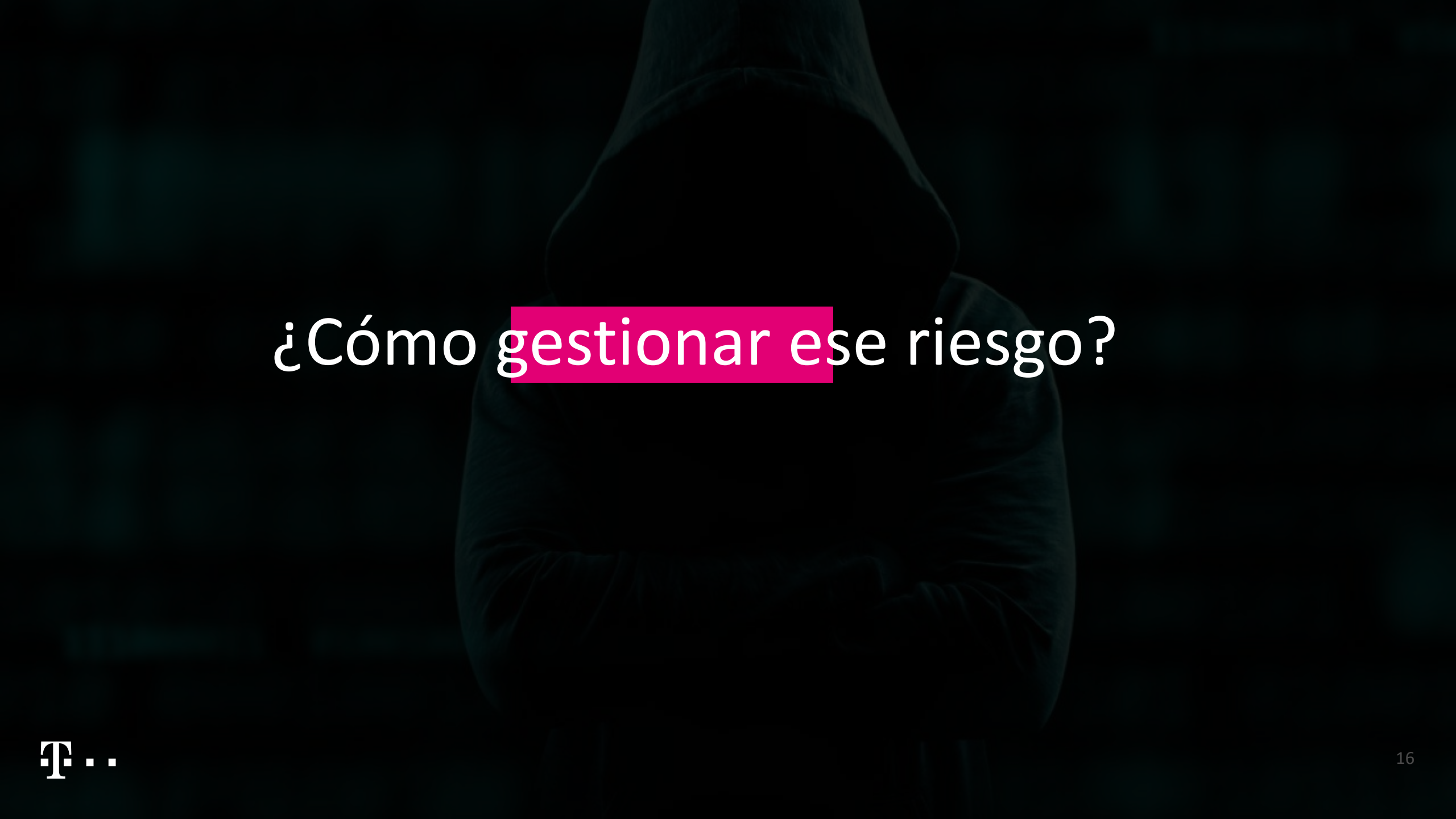
Consecuencias legales

Las leyes de privacidad y protección de datos pueden obligarlo a pagar multas o sanciones reglamentarias debido a:

- Pérdida de datos personales (ejemplo: datos del cliente)
- Falta de medidas de seguridad adecuadas.

RECAPITULANDO…

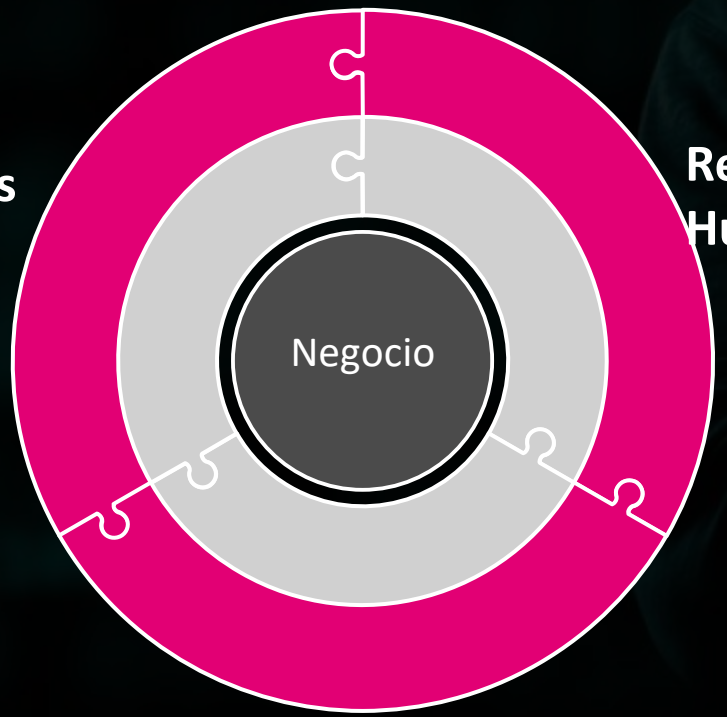
1. Concepto de Ciberseguridad
2. Tamaño del riesgo
3. Sofisticación de ataques
4. Fuentes y Motivantes para un ataque
5. Los impactos que puede causar



¿Cómo gestionar ese riesgo?

NUESTRA METODOLOGÍA

Previo a un ataque → Durante el ataque → Post ataque



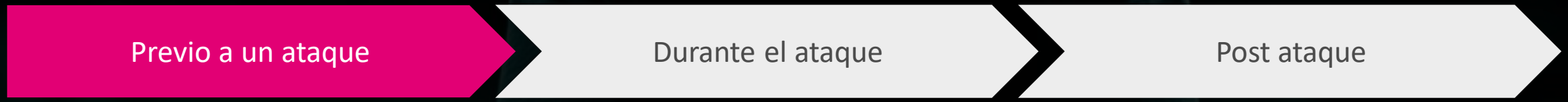
1. Marco organizacional de Riesgos

2. Preparación de la valorización
- Identificar fuentes de amenazas y eventos
- Identificar vulnerabilidades
- Determinar la posibilidad de ocurrencia
- Determinar la magnitud del impacto
- Determinar el riesgo

3. Analisis para priorización de riesgos

4. Planeación de la mitigación, implementación y monitoreo del progreso

NUESTRA METODOLOGÍA



CÓMO SE VE CUANDO INTENTAN IMPLEMENTAR LA SEGURIDAD DESPUÉS DE LA CONSTRUCCIÓN DE LA SOLUCIÓN?

NUESTRA GUÍA PARA HOY

Previo a un ataque | Durante el ataque | Post ataque

- Prevenir y preparar
- Mejores Prácticas
  - Garantizas las capacidades de detección (Procesos internos y externos incluidos para informar.
  - Crear capacidad de respuesta-CERT/CSIRT
  - Capacitar y probar la gestión de crisis y comunicación de crisis.
  - Mejorar la resiliencia de TI y los conceptos de respaldo.
  - Entrenar la conciencia de todos los integrantes de la organización.
  - Configure el gobierno de seguridad y procesos para limitar la superficie del ataque.
  - Habilita capacidades de detección en el mundo exterior

60% de las empresas, son afectadas por Ciber-ataques que distribuyen sus mismos empleados.

- Gestión personal de Contraseñas Seguras
- Adopción de la política de seguridad corporativa
- Verificación de e-mails sospechosos
- Actualiza tu equipo/Verifica tu Antivirus
- Aplica la ley de usar el minimo privilegio de funciones

NUESTRA GUÍA PARA HOY

Ataque previo | Durante el ataque | Post ataque

- Prevenir y preparar
- Mejores Prácticas
  - Garantizas las capacidades de detección (Procesos internos y externos incluidos para informar.
  - Crear capacidad de respuesta-CERT/CSIRT
  - Capacitar y probar la gestión de crisis y comunicación de crisis.
  - Mejorar la resiliencia de TI y los conceptos de respaldo.
  - Entrenar la conciencia de todos los integrantes de la organización.
  - Configure el gobierno de seguridad y procesos para limitar la superficie del ataque.
  - Habilita capacidades de detección en el mundo exterior

- Gestionar, responder y recuperar

NUESTRA GUÍA PARA HOY

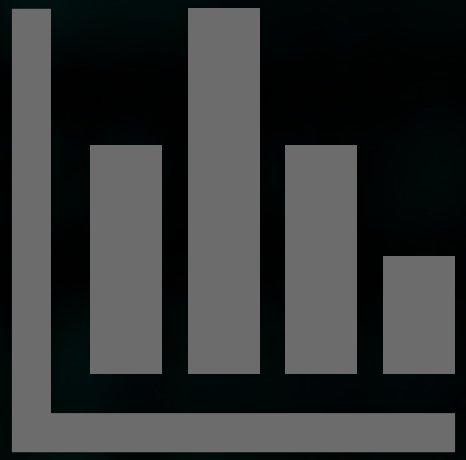
Ataque previo | Durante el ataque | Post ataque

- Prevenir y preparar
- Mejores Prácticas
  - Garantizas las capacidades de detección (Procesos internos y externos incluidos para informar.
  - Crear capacidad de respuesta-CERT/CSIRT
  - Capacitar y probar la gestión de crisis y comunicación de crisis.
  - Mejorar la resiliencia de TI y los conceptos de respaldo.
  - Entrenar la conciencia de todos los integrantes de la organización.
  - Configure el gobierno de seguridad y procesos para limitar la superficie del ataque.
  - Habilita capacidades de detección en el mundo exterior

- Gestionar, responder y recuperar
- Mejores Prácticas
  - Tenga una línea de mando clara.
  - Minimizar el tiempo para resolver /recuperar (MTTR)
  - Deja de buscar culpables.
  - Comunícate cuando tengas que hacerlo. (Interno/Externo)
  - Saber cómo comunicarse a través de los medios.
  - Tratar de mantener tanta evidencia como sea posible (Forense)

Gestión de Crisis

¿CUÁNTOS DÍAS EN PROMEDIO LE TOMA A UNA EMPRESA IDENTIFICAR UNA BRECHA DE SEGURIDAD?



Ve a www.menti.com
y usa el código 28 79 292

Hora de votar

¿CUÁNTOS DÍAS EN PROMEDIO LE TOMA A UNA EMPRESA IDENTIFICAR UNA BRECHA DE SEGURIDAD?

197

Días para detectar

69

Días para contener

NUESTRA GUÍA PARA HOY

Ataque previo

- Prevenir y preparar
- Mejores Prácticas
  - Garantizas las capacidades de detección (Procesos internos y externos incluidos para informar.
  - Crear capacidad de respuesta-CERT/CSIRT
  - Capacitar y probar la gestión de crisis y comunicación de crisis.
  - Mejorar la resiliencia de TI y los conceptos de respaldo.
  - Entrenar la conciencia de todos los integrantes de la organización.
  - Configure el gobierno de seguridad y procesos para limitar la superficie del ataque.
  - Habilita capacidades de detección en el mundo exterior

Durante el ataque

- Gestionar, responder y recuperar
- Mejores Prácticas
  - Tenga una línea de mando clara.
  - Minimizar el tiempo para resolver /recuperar (MTTR)
  - Deja de buscar culpables.
  - Comunícate cuando tengas que hacerlo. (Interno/Externo)
  - Saber cómo comunicarse a través de los medios.
  - Tratar de mantener tanta evidencia como sea possible (Forense)

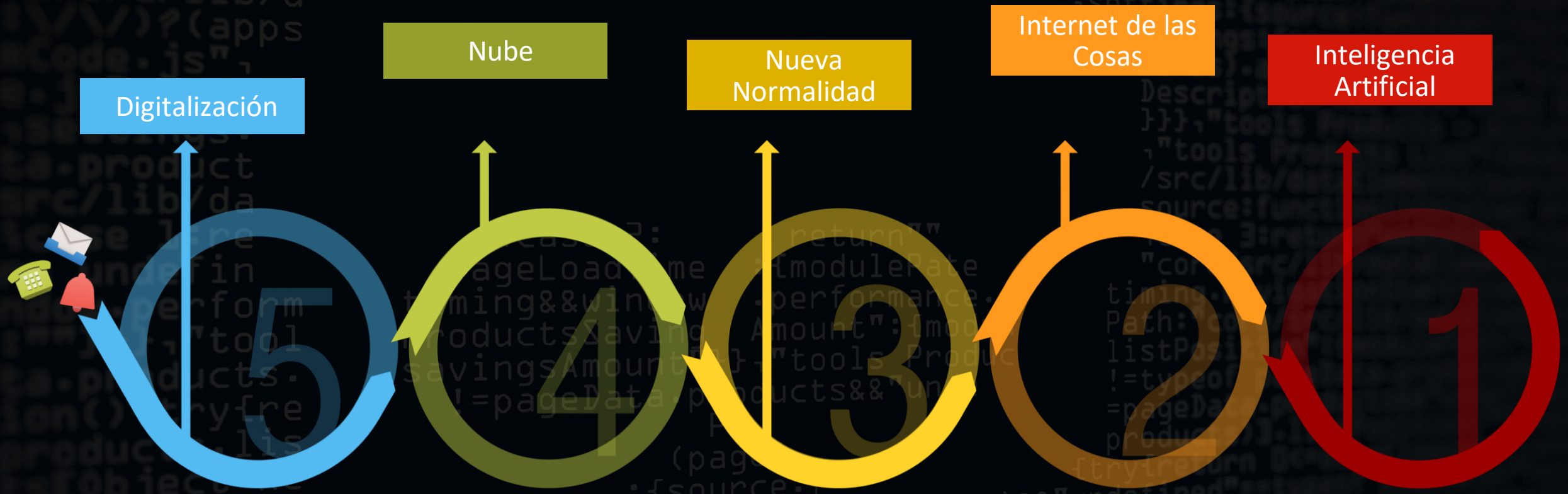
Post ataque

- Aprender y mejorar
- Mejores Prácticas
  - Evaluación de la causa raíz y forense.
  - Realizar una revision Post Mortem
    - ¿Qué funcionó bien?
    - ¿Qué fue lo que no funcionó?
    - ¿Qué se debe de hacer la próxima vez?
    - ¿Qué debería descontinuarse?
  - Mejore su comunicación y gestión de crisis.
  - Asegúrese de prevenir el mismo tipo de incidente en el futuro.

EVOLUCIONEMOS LA SEGURIDAD EN CONJUNTO CON EL NEGOCIO…

UNA COSA MAS…

En una era digital en constante evolución…



…La seguridad es una tarea de todos

T TELEKOM SECURITY

GRACIAS!

Adrian Mata
Adrian.mata@t-systems.com

T Systems