CIBERSEGURIDAD: CÓMO PROTEGER MI EMPRESA

ÍNDICE

1. Introducción

2. Clasificación de ciberataques

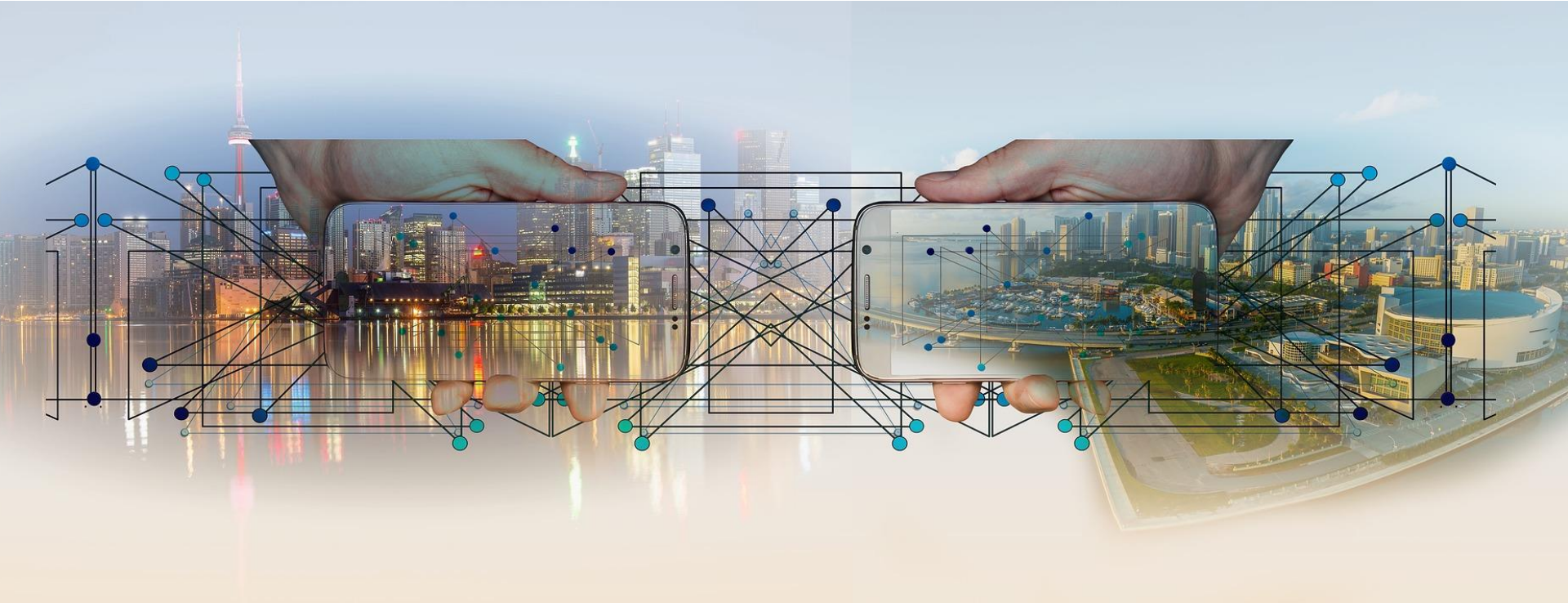
3. Qué hacer ante un ataque

4. Familiarización con la legislación y normativa

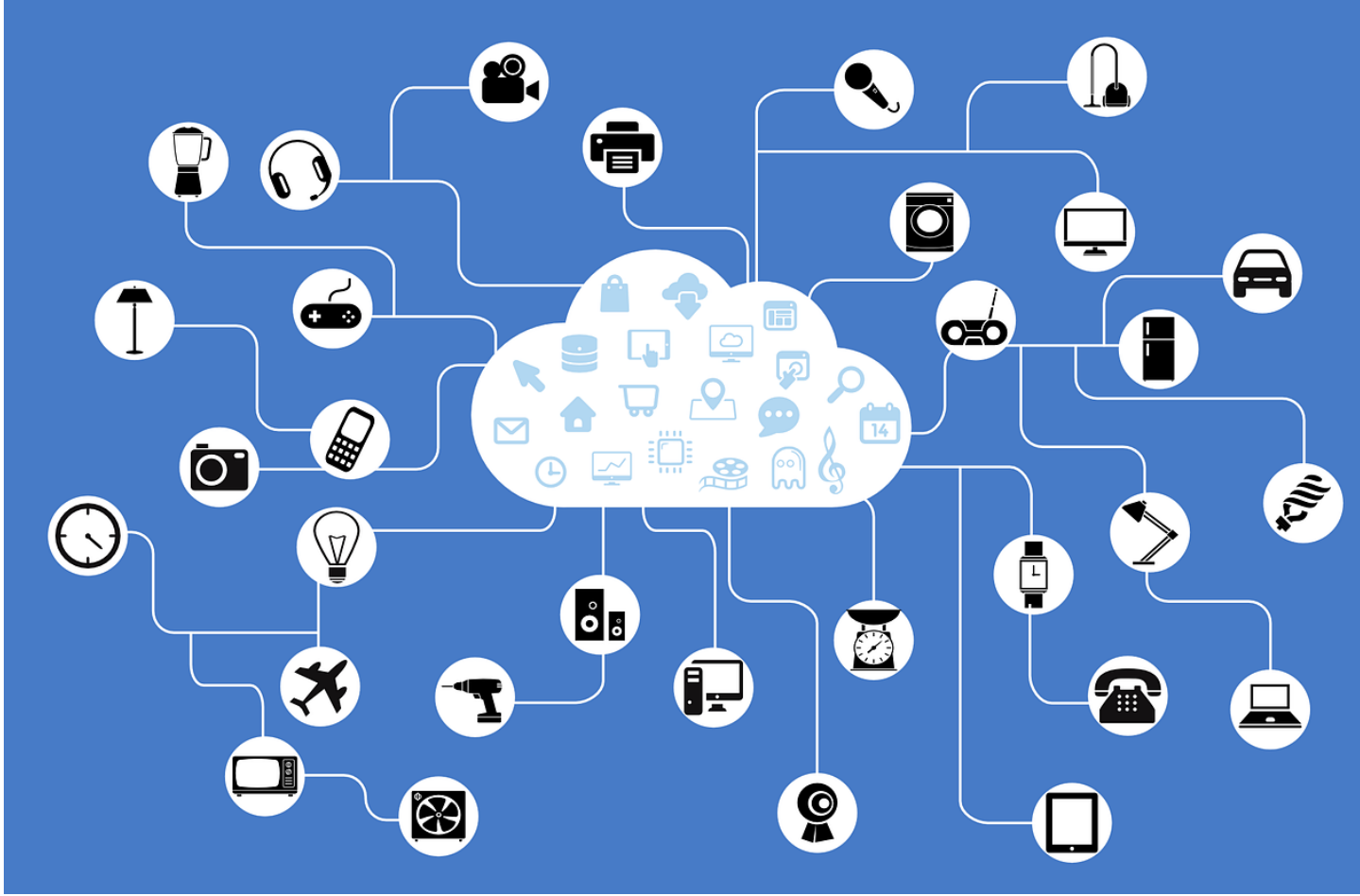
5. Prevención. Creación de una cultura de ciberseguridad en el trabajo

1. INTRODUCCIÓN

SITUACIÓN ACTUAL



Internet de las Cosas



ALGUNOS DATOS DE 2016

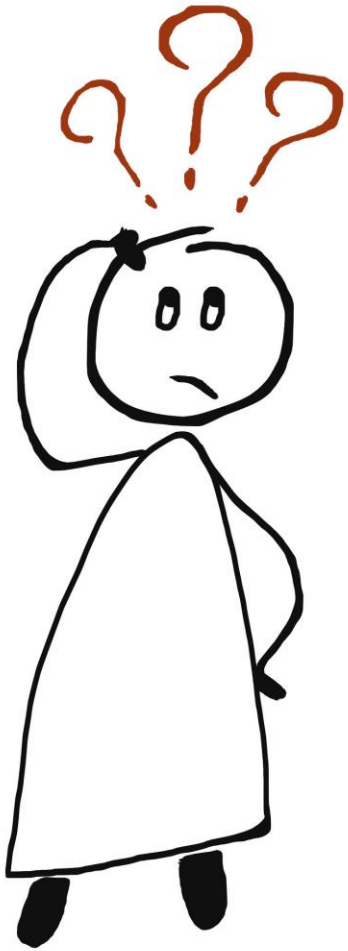
- CCN-CERT gestionó más de 20.000 ciberincidentes, detectados principalmente en el sector público y en empresas, lo que supone un 14,5% más que en 2015
- De ellos, el 3,6% fueron catalogados como muy altos o críticos
- Solo en España se trataron más de 2.000 incidentes de distintos tipos de ransomware, un 375% más que en 2015
- Los ataques de denegación de servicio registrados solo en el segundo trimestre de 2016, se incrementaron en un 129% más que los registrados en el mismo trimestre de 2015

Fuente: Ciberamenazas y Tendencias (Edición 2017) del Centro Criptológico Nacional (CCN)

¿Y EN 2017?

- INCIBE ha resuelto más de 120.000 incidentes de seguridad en 2017, un 6,77% más que 2016
- De estos incidentes, más de 100.000 afectaron a empresas y ciudadanos, 885 a operadores estratégicos y 5.537 correspondieron al ámbito académico de la RedIRIS

Fuente: Balance 2017 del Instituto Nacional de Ciberseguridad (INCIBE)



¿QUÉ ES CIBERSEGURIDAD?

Es la disciplina que se encarga de que los sistemas de información sean seguros y confiables.

Los sistemas de información son la información y todo lo que la gestione o contenga.

BENEFICIOS

Proteger nuestra información.

Garantizar la disponibilidad de nuestros servicios.

Obtener la confianza de nuestros clientes.

Evitar robos y fugas de datos.

Estar preparados para continuar con nuestra actividad en caso de que ocurra un incidente.

Prevenir incidentes.

Evitar pérdidas de reputación.

Cumplir con la legislación.

Fuente: Instituto Nacional de Ciberseguridad (INCIBE)

2. CLASIFICACIÓN DE CIBERATAQUES

LOS MÁS CONOCIDOS

Malware

- Software malicioso cuyo objetivo es infiltrarse en un sistema para dañarlo.
- Virus, gusanos, troyanos, etc.

Phishing

- Robo de datos personales, bancarios, etc.
- Funcionan mediante la suplantación de identidad.
- Se realiza a través del correo electrónico, mensajería o llamadas telefónica.

Denegación de Servicio (DoS)

- Consiste en realizar un número considerable de peticiones a un servidor.
- El objetivo es colapsar y saturar un sistema.
- La técnica más habitual es infectar múltiples dispositivos para poder utilizarlos en el ataque.

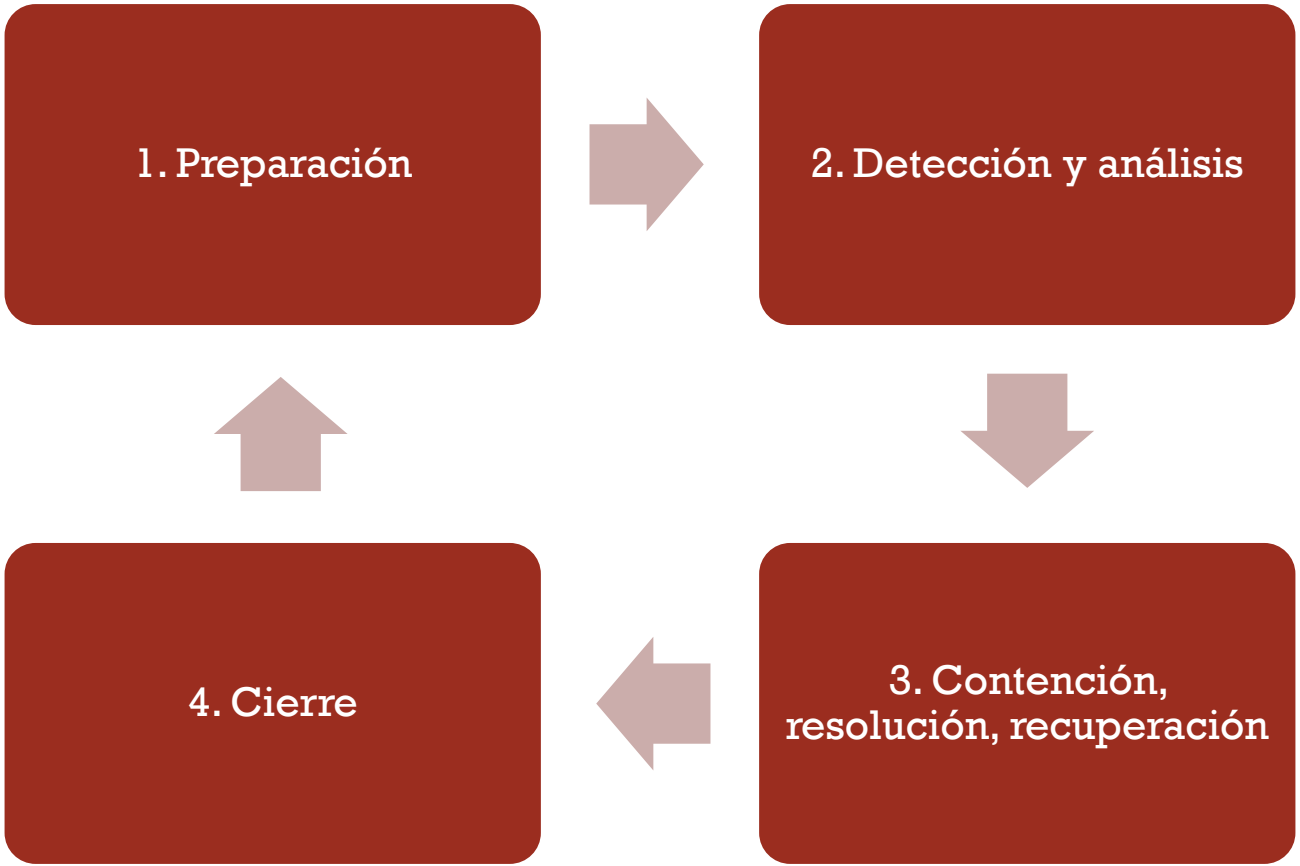
Exploit

- Programa que aprovecha una vulnerabilidad
- Múltiples objetivos: robar, espiar, controlar o modificar la configuración de los dispositivos, etc.

COSTE DE UN CIBERATAQUE

- Tiempo de inactividad
- Costes económicos
- Pérdidas de datos
- Daños de reputación

3. QUÉ HACER ANTE UN ATAQUE


1. Preparación
2. Detección y análisis
3. Contención, resolución, recuperación
4. Cierre

FASE 1 - PREPARACIÓN

- Estimar las necesidades para la gestión del incidente
- Definición de política de gestión de incidentes
- Catálogo con las incidencias más probables

FASE 2 – DETECCIÓN Y ANÁLISIS

- Identificación
- Clasificación y priorización
- Notificación

FASE 3 – CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

- Contención
  - Varía según el tipo de incidente y el impacto
  - Más eficaz si previamente se han definido estrategias
- Resolución
  - Recuperación de los sistemas afectados
- Recuperación
  - Eliminación de los componentes asociados al incidente

FASE 4 - CIERRE

- Documentar la gestión del incidente
- Registro común de incidentes
- Revisión periódica de las estrategias
- Analizar y medir

¡LO MÁS IMPORTANTE!

¿Has sufrido un incidente?

- Cuenta con la ayuda de expertos
- Contacta con INCIBE

Cualquiera puede reaccionar ante un ciberataque, la cuestión es adaptar la metodología según los recursos con los que se cuente.

4. FAMILIARIZACIÓN CON LA LEGISLACIÓN Y NORMATIVA

EL PANORAMA LEGAL ACTUAL

- Legislación y normativa bastante extensa
- Leyes de ámbito estatal y europeo
- Existen organismos internacionales que generan normas y estándares

Conocer y cumplir las leyes y los estándares ayuda a mejorar la seguridad de nuestra empresa.

BENEFICIOS

- Mejora la gestión de la seguridad de la empresa
- Mayores garantías de seguridad y niveles de servicio
- Mejora la reputación
- Ayuda a identificar los riesgos y vulnerabilidades
- Refuerza la aplicación de buenas prácticas de seguridad
- Evita sanciones
- Evita problemas con terceros

PRINCIPALES LEYES

LOPD

(Ley Orgánica de Protección de Datos)

- Protección de datos personales
- Nivel de protección dependiente de sensibilidad del dato
- Cambio a RGPD (mayo 2018)
- Organismo responsable la Agencia Española de Protección de Datos

LSSI

(Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico)

- Personas/empresas que realicen actividades económicas por Internet
- Obligatorio cumplir una serie de exigencias, por ejemplo, en la página web

PRINCIPALES LEYES

LGT

(Ley General de Telecomunicaciones)

- Operadores de telecomunicaciones
- El objetivo es la regulación

LPI

(Ley de Propiedad Intelectual)

- Protección de los derechos de autor de todo tipo de creaciones
- Obligatorio (si procede) pagar licencias de software, reconocer autorías, etc.

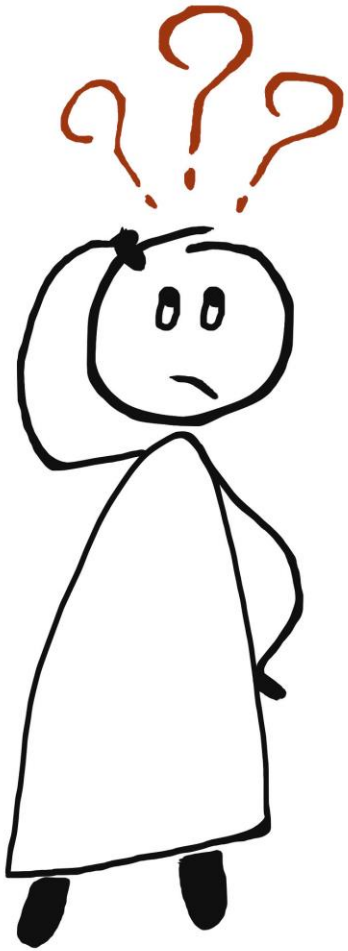
ESTÁNDARES INTERNACIONALES

- ISO/IEC 27000 SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
  - ISO 27001:2013: Sistemas de Gestión de la Seguridad de la Información (SGSI)
  - ISO 27002:2005: Código de buenas prácticas para la Gestión de la Seguridad de la Información
  - ISO 27005:2011:Gestión de riesgos de seguridad de la información
  - ISO 27032:2012: Directrices de ciberseguridad
  - ISO 27035:2011: Guía de gestión de incidentes de Seguridad

5. PREVENCIÓN. CREACIÓN DE UNA CULTURA DE CIBERSEGURIDAD EN EL TRABAJO

NIVEL DE PROTECCIÓN BÁSICO

- No proporcionar datos confidenciales, bancarios, contraseñas, etc.
- No instalar programas de origen desconocido
- Prestar atención a las URL cuando se navega
- No abrir enlaces sospechosos ni descargar archivos adjuntos
- En los emails fijarse en la dirección de correo del remitente



¿CÓMO PUEDO PROTEGER MI EMPRESA?

Puestos de trabajo

Comunicaciones

Dispositivos móviles

PUESTOS DE TRABAJO

- Uso de antivirus
- Cifrado de datos
- Copias de seguridad
- Control de contraseñas
- Bloqueo del ordenador
- Política de mesas limpias
- Política de uso de los sistemas

COMUNICACIONES

- Redes privadas virtuales (VPN)
- Cortafuegos
- Política de uso del correo electrónico
- Técnicas para telefonía IP

DISPOSITIVOS MÓVILES

- Bloqueo del terminal
- Cifrado de datos
- Copias de seguridad
- Software actualizado
- Aplicaciones de confianza
- No utilizar WiFis públicas

Nuestros empleados son nuestros mejores aliados en materia de prevención.

LA CIBERSEGURIDAD ES COSA DE TODOS

¡GRACIAS!

@Uppertechnology

www.uppertechnology.com

contact@uppertechnology.com