Retos/apuesta de la Transformación Digital en el Ayuntamiento de Calvià: Gobierno del dato, ciberseguridad e IA


Transformación Digital
Administración Electrónica
39/2015
Big data
IA
40/2015
Smart city
Wi-Fi
Preservación digital
Gobierno del dato
Gestión documental
IT
Ciberseguridad

ESCENARIO DE PARTIDA

Lo URGENTE quita tiempo para lo IMPORTANTE

Prima la USABILIDAD a la seguridad

Entorno cada vez más digital

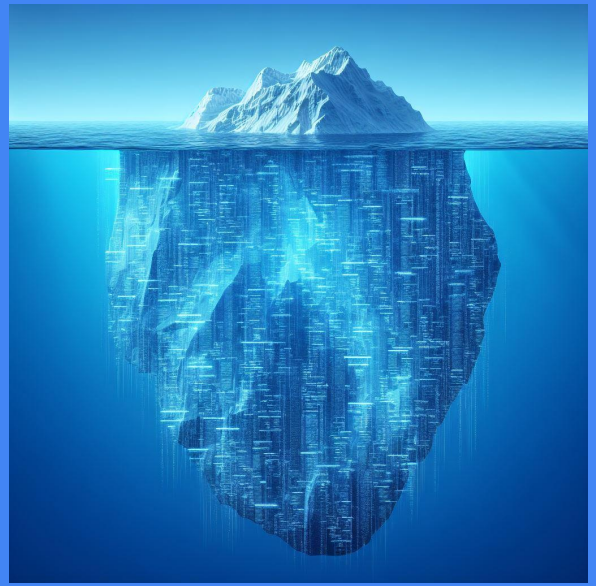
Recursos limitados

Poco tiempo disponible para prácticas recomendadas / actualizaciones

ESCENARIO DE PARTIDA

La seguridad al 100% no existe

Los casos que trascienden solamente son la punta del iceberg



La pregunta a formularse NO es:
¿Seremos víctimas de un ciberataque?
Sino: ¿**Cuándo nos ciberatacaran?**

Se espera que el ransomware ataque a una empresa, un consumidor o un dispositivo cada **dos segundos el año 2031**

ESCENARIO DE PARTIDA

Alcampo sufre un ciberataque que afecta a su operativa habitual

Madrid - 28 AGO 2024 - 20:40 CEST

Repsol sufre un ciberataque a su base de datos de clientes de electricidad y gas en España

EL PAÍS

19 SEPT 2024 - 19:03 | Actualizado: 19 SEPT 2024 - 19:30 CEST

13E

MAÑANA DEL 13E

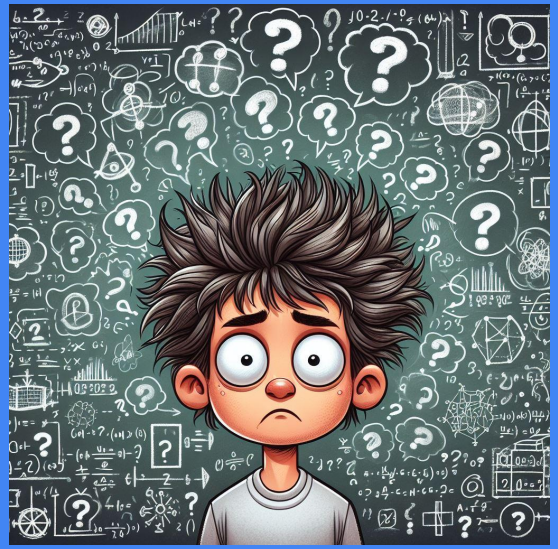
Detección

Desconexión TOTAL de los sistemas y redes

Contacto con los servicios de CSIRT

Constitución del comité de crisis

Comunicado a las autoridades competentes



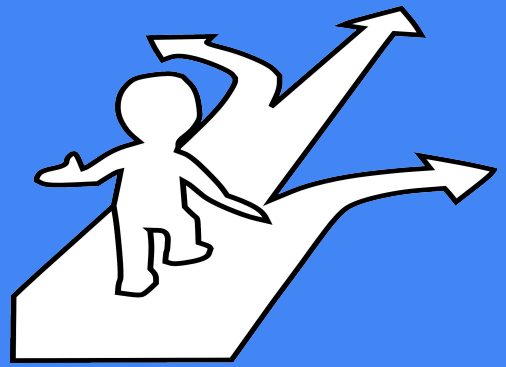
Apuesta por la TRANSPARENCIA desde el primer momento

DÍAS POSTERIORES

Necesidad de seguir trabajando

Papel decisivo WiFi y cloud

Implicación de las personas usuarias

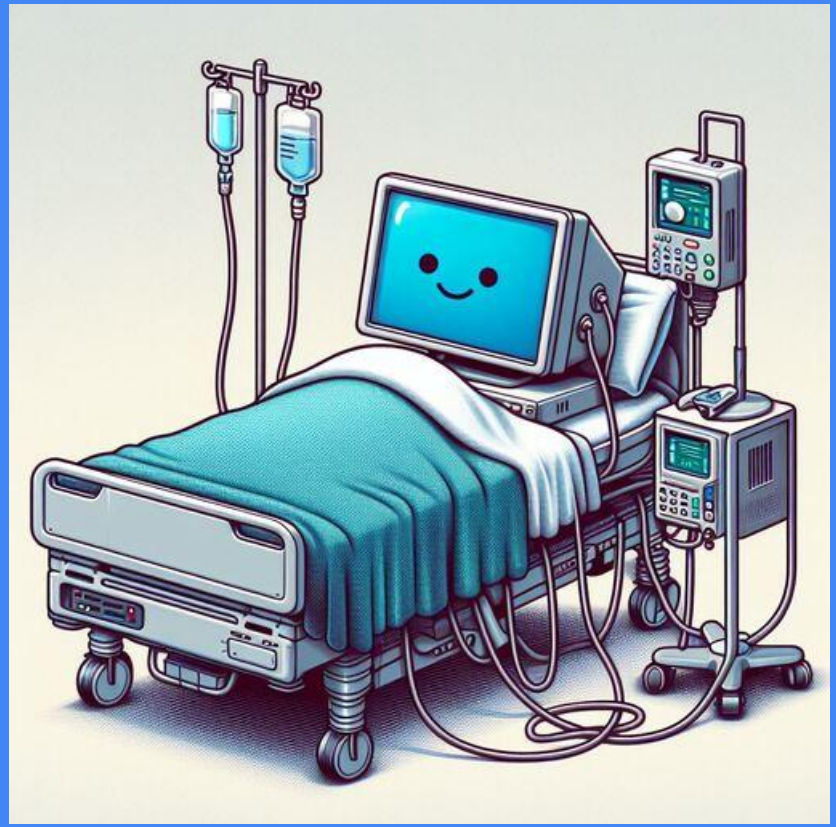


Análisis forense

Verificación de backups

Cambios de prioridades constantes

FASE DE RECUPERACIÓN



PREMISA: Todo lo que conforme la nueva RED LIMPIA deberá estar ACTUALIZADO y bastionado con un grado elevado de SEGURIDAD.

FASE DE RECUPERACIÓN

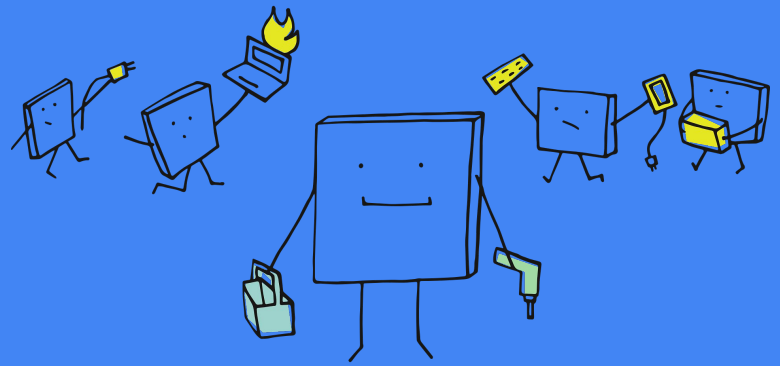
Bastionado y clasificación de los sistemas en:
ACTUALIZABLES / PRESCINDIBLES / LEGACY

Recuperación paulatina en función viabilidad / impacto / facilidad

Prioridades marcadas por el comité de crisis

Cambio masivo de credenciales

Recursos propios



FASE DE RECUPERACIÓN

ALGUNAS AMENAZAS

Zona de confort

Resistencia al cambio (usuarios finales y técnicos)

“*Siempre se ha hecho así*”

Falta de perspectiva / Necesidad de apoyarse en partners

Presupuesto

Rigidez de contratación en la Administración

NO HAY MALWARE QUE POR BIEN NO VENGA

ASPECTOS POSITIVOS DEL CIBERATAQUE

Tiempo

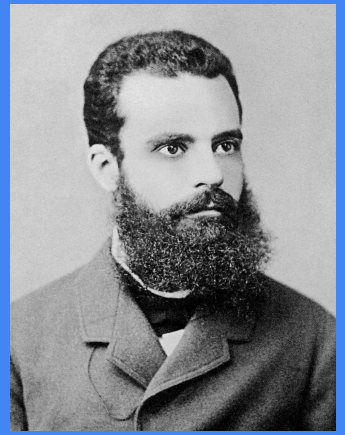
Menor resistencia a nuevas medidas de seguridad

Sistemas y redes actualizados y más seguros

Motivación del equipo

¿POR DÓNDE EMPEZAR?

Con POCO se puede conseguir MUCHO:



- Política de contraseñas seguras
- Copias de seguridad inmutables / no conectadas
- Restricción uso dispositivos de almacenamiento USB
- Seguridad del endpoint
- Orígenes geográficos
- Horarios de navegación
- MFA
- Actualizaciones periódicas
- Protección de navegación / correo

ALGUNOS CONSEJOS

Seguridad transversal como mejora continua (entorno cambiante)

Enfocar como proyecto por fases y PRIORIZAR

Pasar de preocuparse a OCUPARSE

Sustituir sistemas legacy

Actualizaciones periódicas

ALGUNOS CONSEJOS

Formación e información:

concienciación de Responsables, Técnicos y Usuarios finales

Brindar herramientas seguras a los usuarios

Apoyarse en asistencia técnica especializada

Ante recursos limitados:

Automatización / Delegación

Importancia de realizar auditorías / simulacros

GRACIAS