Tecnologías de privacidad mejorada (PETs) en: Sistemas Windows y Redes Microsoft

Genís Margarit (gmargarit@centralip.net)
@gmargarit

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Introducción

- Sistemas operativos continúan siendo mayoritariamente **Windows**
- Para resumirlo, mi experiencia lo vincularía al éxito del **Microsoft Office**

Genís Margarit (gmargarit@centralip.net)
@gmargarit

De la LOPD al GDPR

- En **LOPD**
  - Las entidades tenían todas las obligaciones
  - Instrucciones concretas (por ej. copia de seguridad semanal)
  - Limitaban la promoción de PETs
- En **GDPR**
  - Los **PIA** provocan análisis de riesgos
  - Con lo anterior aparecen las **PETs**
- Evolución de la figura del experto
- Rendición de cuentas entre cliente y proveedor

Genís Margarit (gmargarit@centralip.net)
@gmargarit

Evolución de la figura del experto

- Los **análisis de riesgos** provocan un papel en blanco
- Un elevado conocimiento de los entornos para promover todas las **medidas que están al alcance**
- Por ejemplo, infraestructuras de clave pública y privada y su impacto en redes, sistemas y aplicaciones
- El GDPR sacude a los expertos en privacidad

Genís Margarit (gmargarit@centralip.net)
@gmargarit

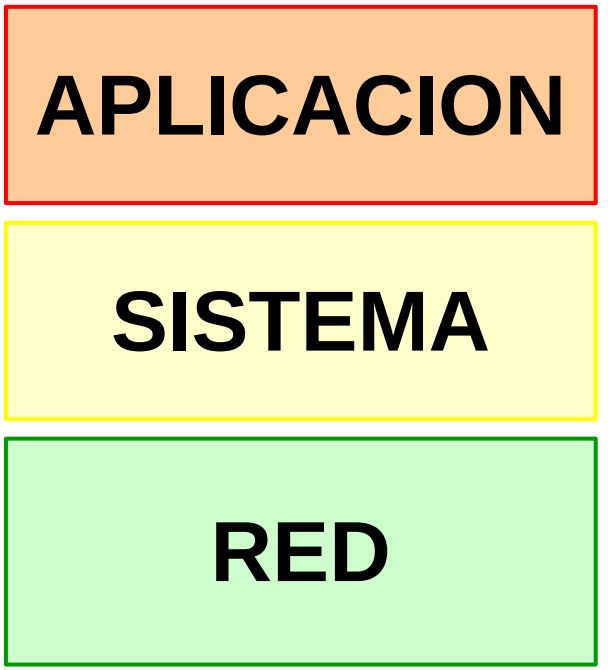
Rendición de cuentas entre cliente y proveedor

- Mercado más exigente y penalización de la ausencia de PETs
- Como proveedores han presupuestado horas adicionales de proyectos?
- Cuales acabaran siendo los **sellos** de los servicios/productos/tecnologías y cuales las **certificaciones** de los expertos?

Genís Margarit (gmargarit@centralip.net)
@gmargarit

Conocimiento de las medidas de seguridad de Microsoft

- Empezar por las **redes**
- Pasando por los **sistemas**
- Terminando en las **aplicaciones**



Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

PETs en la capa de red

- Control de acceso a la red
- Comunicaciones secretas con IPSec
- *Firewall* avanzado de Windows
- Servicios de red
  - Servicio DHCP
  - Servicio DNS
  - Servicio de acceso remoto
    - Servicio de red privada virtual (VPN)
    - Servicio de escritorio remoto

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

Control de acceso a la red

- **Network Policy Server** (NPS)
- Políticas basadas en condiciones
- Pueden incorporarse atributos de sistema operativo
- Sistema de **cuarentenas** y redes de **vacunas**

Genís Margarit (gmargarit@centralip.net)
@gmargarit

Comunicaciones secretas IPSec

APLICACION

SISTEMA

RED

- Comunicaciones con integridad y seguridad
- Configuración masiva y desatendida
- Autentificación de los nodos mediante **Kerberos**

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

Firewall avanzado de Windows

- Estigma del mal recuerdo del primer *firewall* de Windows
- El *firewall* actual permite filtrar:
  - Tráfico de entrada y salida
  - **Ámbitos** (hogar, público, trabajo)
  - Usuarios y equipos
  - IP@, *socket* origen y destino
  - **Registros**

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

Servicios de red

- Servicio DHCP
  - Reservas de configuraciones
  - **Listas de MAC permitidas** y así recibir alertas o prohibir nodos desconocidos
- Servicio DNS
  - **DNSSec** para evitar *spoofing*
  - ***Locking* de la caché** para evitar el caché *poisoning*
  - ***Split* DNS** para asegurar resoluciones corporativos contra los servidores internos

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

Servicio de acceso remoto

- Servicio de red privada virtual (VPN)
  - **DirectAccess** en segundo plano
  - Túnel cuando inicia el sistema operativo
  - Políticas inmediatas (incluyendo desmantelamiento)
  - **SSTP** salta *proxies* y *firewalls*
- Servicio de escritorio remoto
  - **RDP Gateway** maquilla todo el tráfico como https

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

PETs en la capa de sistema

- Mejoras en la autentificación
- Privacidad en el bloqueo y desbloqueo
- Control de dispositivos
- Permisos de instalación
- Conclusión de la capa de sistema

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

Mejoras en la autentificación

- Contraseñas
  - **GPOs** asigna a equipos (problemática)
  - **PSOs** asigna a usuarios
  - **Windows Azure Active Directory**
    - Segundo factor mediante **OTP**
    - Renovar o recuperar mediante **OTL**

Genís Margarit (gmargarit@centralip.net)
@gmargarit

Privacidad en el bloqueo y desbloqueo

APLICACION

SISTEMA

RED

- Protector de pantalla
  - Manual o automático per confederado al servidor
  - Difundir funciones y obligaciones de privacidad
- **Bitlocker** para cifrar discos duros
  - Integración con todos los Windows
  - Transportar discos sin riesgo de pérdida o robo
  - Cifrar con **TPM** para anclar a un equipo
  - Ausencia de: destrucción o borrado remoto, doble fondo, contraseña de señuelo o geofencing

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

Control de dispositivos

- **Lista blanca de dispositivos**
  - Identificados mediante su dirección física
- Aparato que no aparece en el inventario
  - Bloqueado o **generación de alerta**
  - Protección de *malaware* y *keyloggers*

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

Permisos de instalación

- Pesadilla de aplicaciones con permisos elevados para los usuarios
- Usuarios sin privilegios que pueden instalar en sus carpetas personales
  - Por ejemplo impacto de Dropbox, GDrive, etc.
- **Applocker**
  - Permite bloquear la **ejecución** de programas no autorizados
  - Perfecto para combatir el ***ransomware***

Genís Margarit (gmargarit@centralip.net)
@gmargarit

APLICACION

SISTEMA

RED

PETs en la capa de aplicación

- La copia de seguridad de la información
- El almacenamiento de la información
- Intercambios seguros de documentación
- Conclusiones de la capa de aplicación

Genís Margarit (gmargarit@centralip.net)
@gmargarit

La copia de seguridad de la información

APLICACION

SISTEMA

RED

- **Windows Backup** permite
  - Incluso con ficheros abiertos
  - Unidades de información son pequeños trozos del sistema de ficheros (*chunks*)
  - ***Shadow Copies*** para histórico de versiones
  - Destino en un lugar distinto (OneDrive o Azure)
    - Con los *chunks* sincroniza y copia en tiempo real

Genís Margarit (gmargarit@centralip.net)
@gmargarit

El almacenamiento de la información

APLICACION

SISTEMA

RED

- **Work folder** y **OneDrive** siempre accesibles des de cualquier dispositivo (Android, IOS, etc.)
- **Storage groups** para RAID sencillos y baratos
- **Hyper-V Replica** para alta accesibilidad
- **FSRM** para
  - Clasificar en función de contenido, antigüedad, última vez, etc.
  - Ficheros se van moviendo automáticamente para ir a las ubicaciones más seguras

Genís Margarit (gmargarit@centralip.net)
@gmargarit

Intercambios seguros de documentación

APLICACION

SISTEMA

RED

- Evitar que la seguridad se pierda cuando se copia a un USB, adjunta a un mail, se cuelga en Dropbox, etc.
- Derechos digital (**DRM**) de Office asignan permisos de leer, editar, copiar, imprimir o fechas de caducidad al fichero
  - Estos permisos serán independientes por dónde se distribuya o mueva el documento

Genís Margarit (gmargarit@centralip.net)
@gmargarit

Conclusión final

APLICACION
Windows Backup, Shadow Copies
FSRM, OneDrive o DRM

SISTEMA
PSOs, Windows Azure AD
Bitlocker, polítiques USB y Applocker

RED
NPS, IPSec, WAF, DHCP list,
DNSSec, DirectAccess y RDP Gateway

Genís Margarit (gmargarit@centralip.net)
@gmargarit