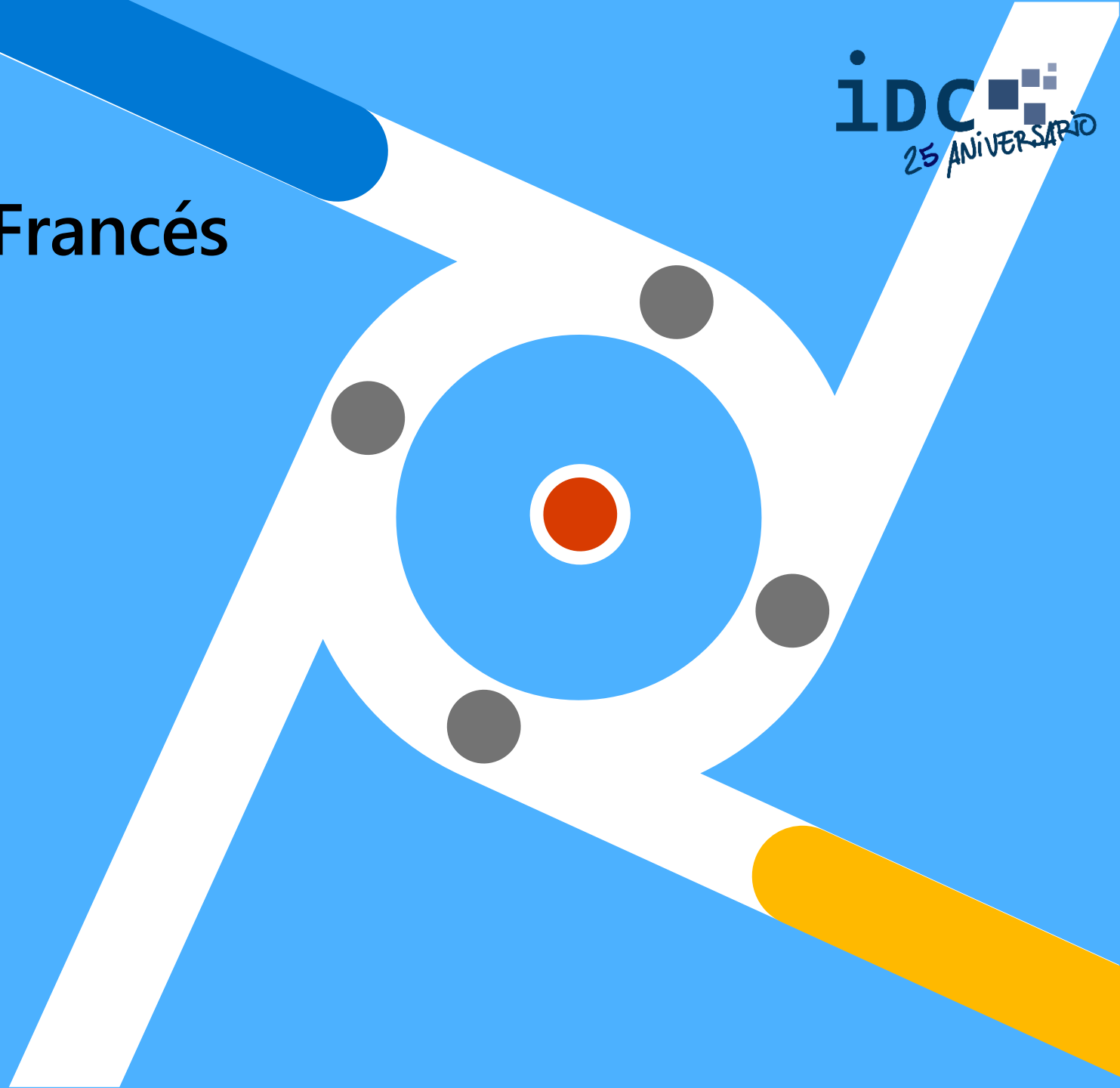
Microsoft Security

Ciberataque en el Liceo Francés

Aurore Dhuez
Responsable del departamento de Nuevas Tecnologías del Liceo Frances de Valencia

Cecilio Rodríguez
Director Comercial de IDC

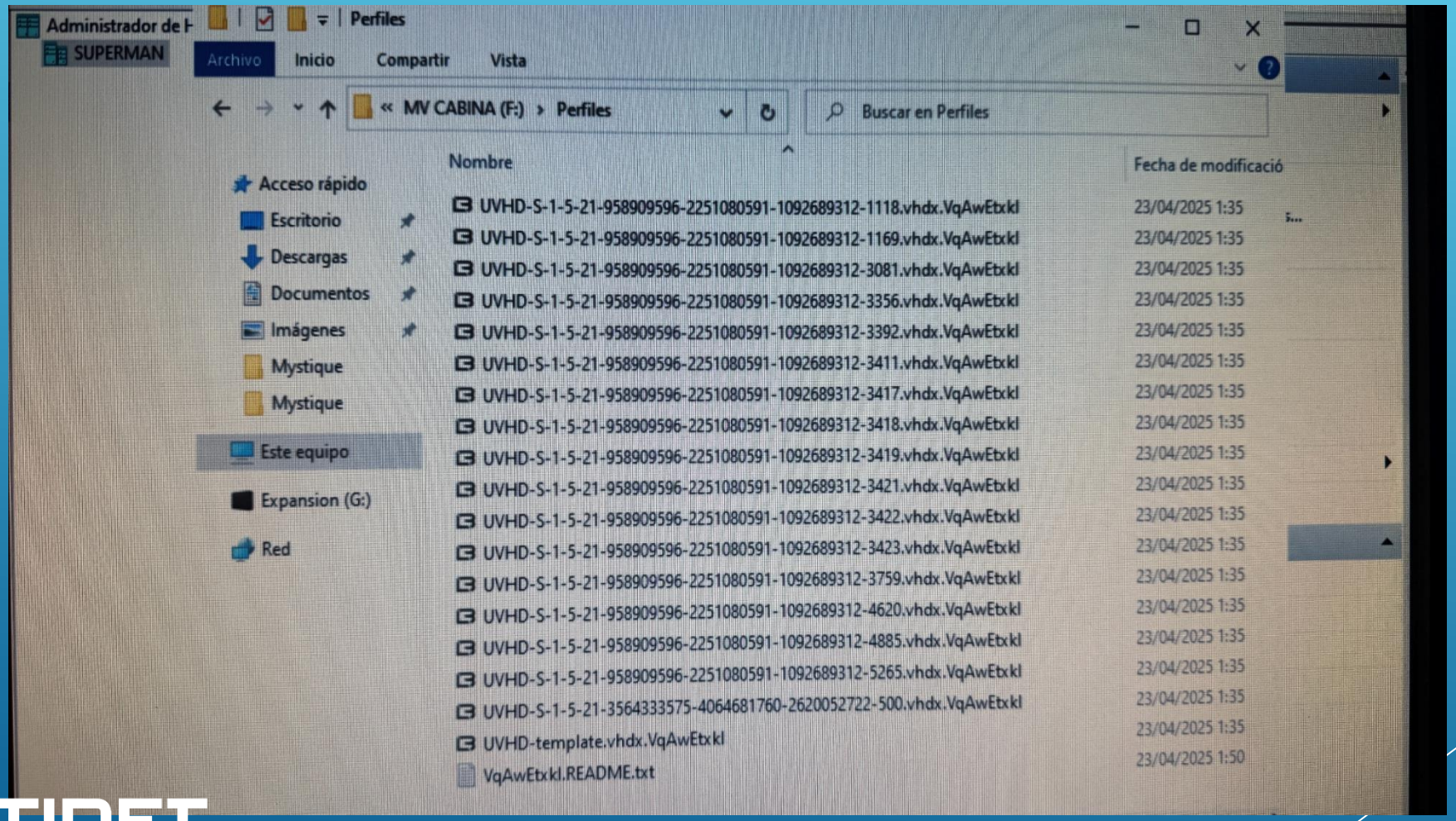
Enrique Fuster
Director Técnico de IDC



FORTINET

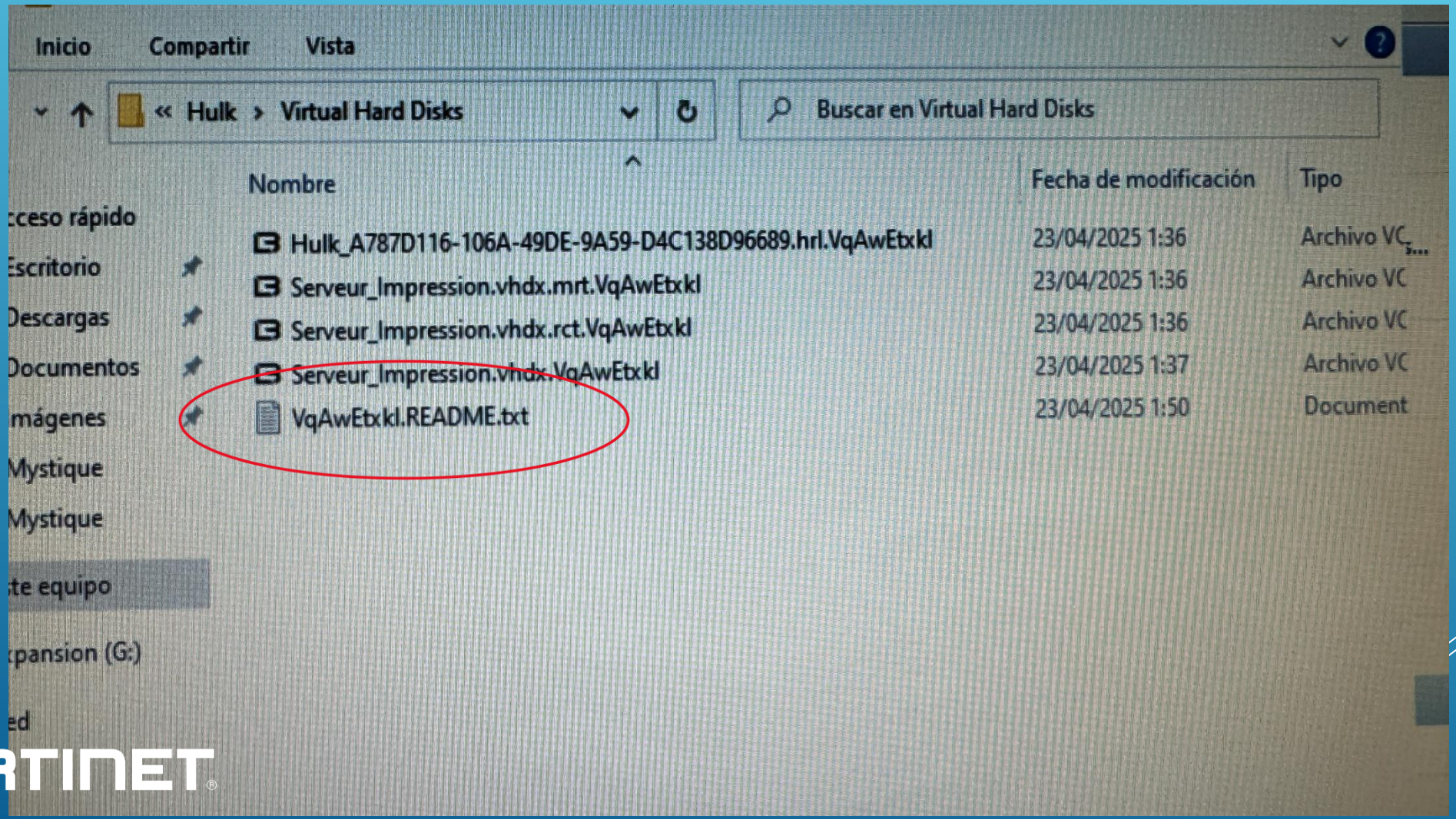
DETECCIÓN Y EVALUACIÓN INICIAL

Detección mediante usuario que alerta al Departamento de TI que evalúa la situación.



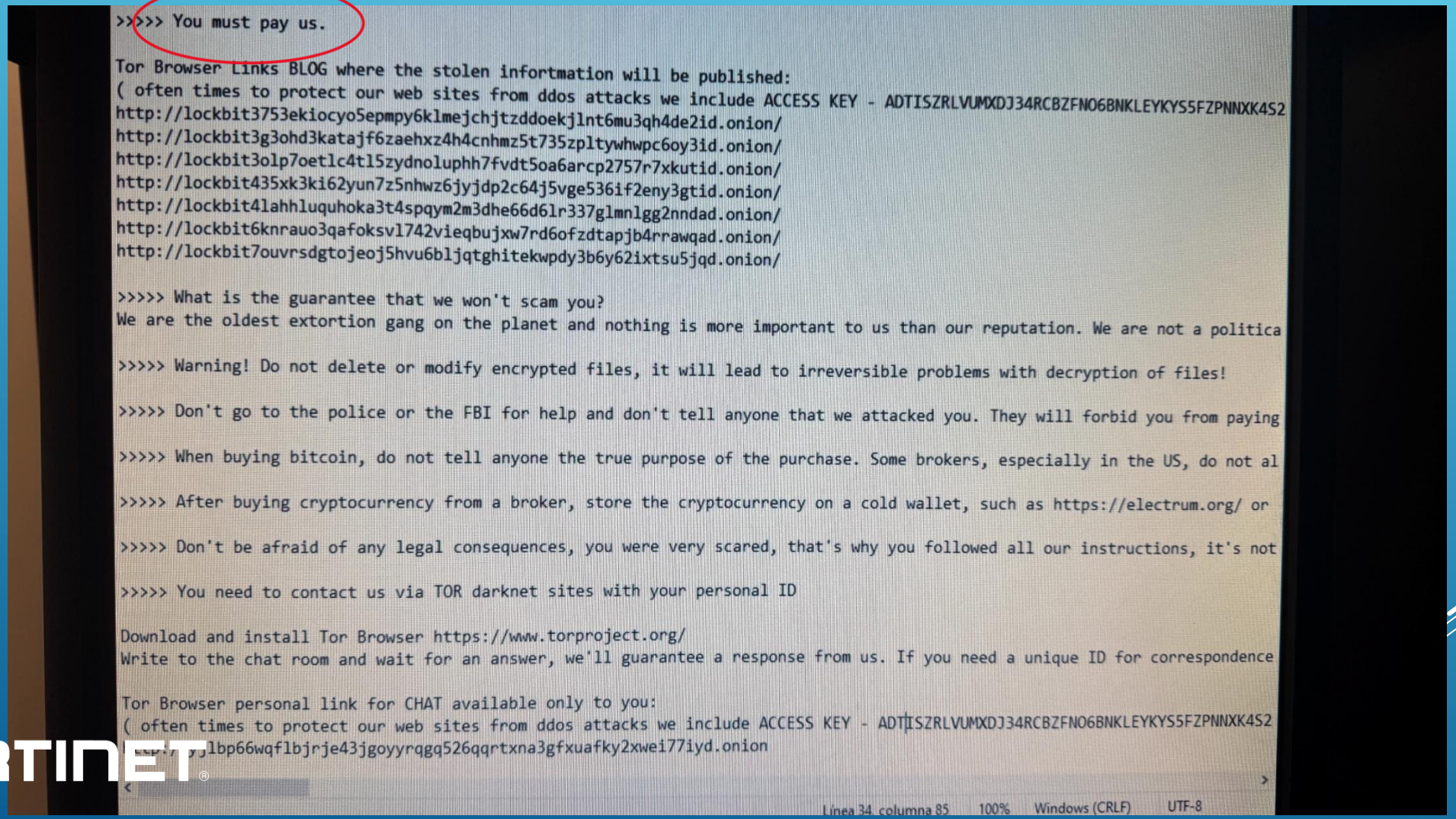
DETECCIÓN Y EVALUACIÓN INICIAL

Evaluación inicial mediante un acceso físico.



DETECCIÓN Y EVALUACIÓN INICIAL

Confirmación de ataque dirigido y demanda de dinero para recuperar los datos.



COORDINACIÓN Y RESOLUCIÓN

El personal del departamento contacta con IDC el mismo día y en ese momento se designa un equipo de crisis que consta de:

- **Coordinador de proyecto**: Realizará las funciones de coordinación del proyecto y enlace con el departamento de informática del Liceo.

- **Técnico experto en sistemas** para que evalúe los daños e inicie la restauración del sistema y lleve a cabo la puesta en producción del mismo de nuevo.

- **Técnico experto en comunicaciones**, que analice el ciberataque y rehaga de nuevo las comunicaciones y las ponga en producción.

DETECCIÓN Y EVALUACIÓN INICIAL

El comité de crisis designado empieza el trabajo de reconstrucción:

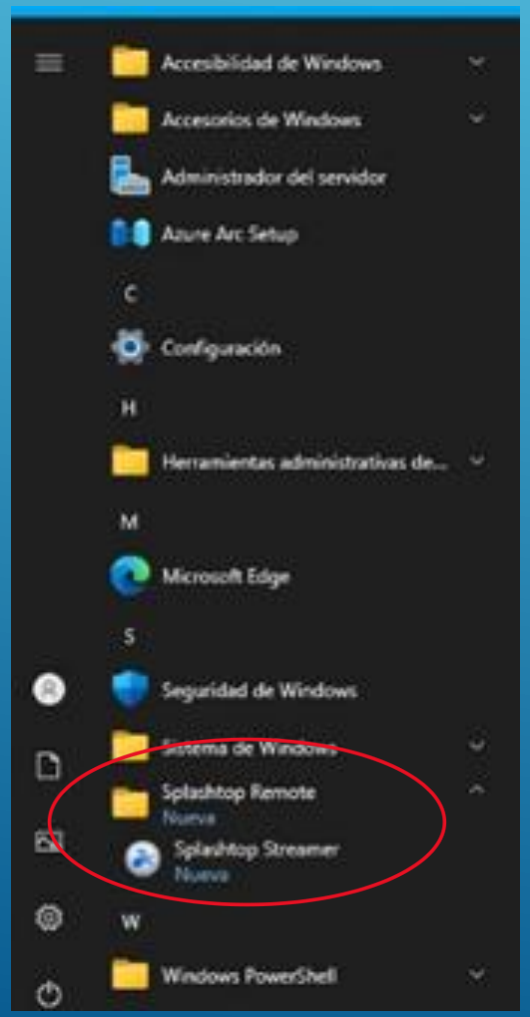
- *Tareas administrativas*; comunicación de la brecha de seguridad al DPO para la apertura de incidencia en AEPD, denuncia en la Guardia Civil y comunicación a trabajadores y resto de implicados.

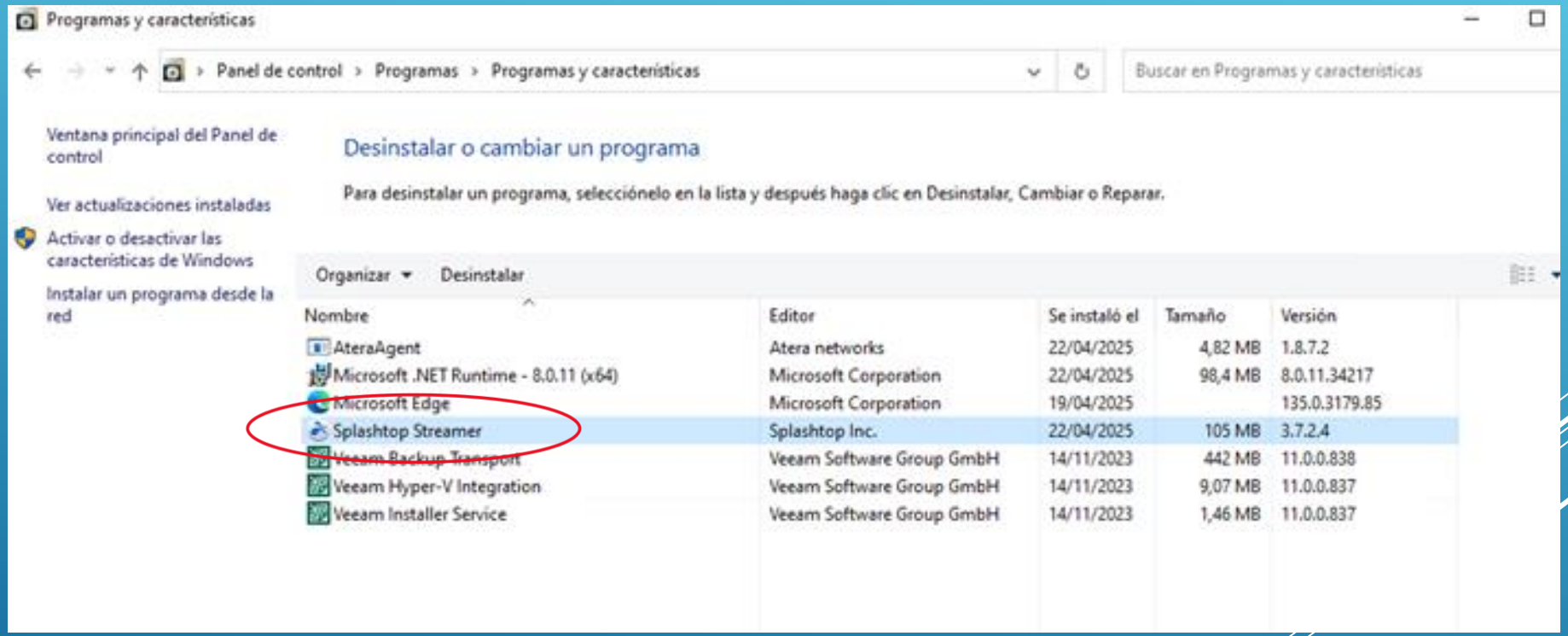
- *Plan de restauración* diseñado por parte del Técnico *de sistemas*, evaluación de daños, comprobación de medidas reactivas, e inicio de la restauración del sistema.

- *Plan de restauración* diseñado por parte del Técnico *de comunicaciones*, creación de segmento limpio para sistemas, análisis del ciberataque y reorganización de las comunicaciones y puesta de nuevo en producción.

ANALISIS DEL CIBERATAQUE

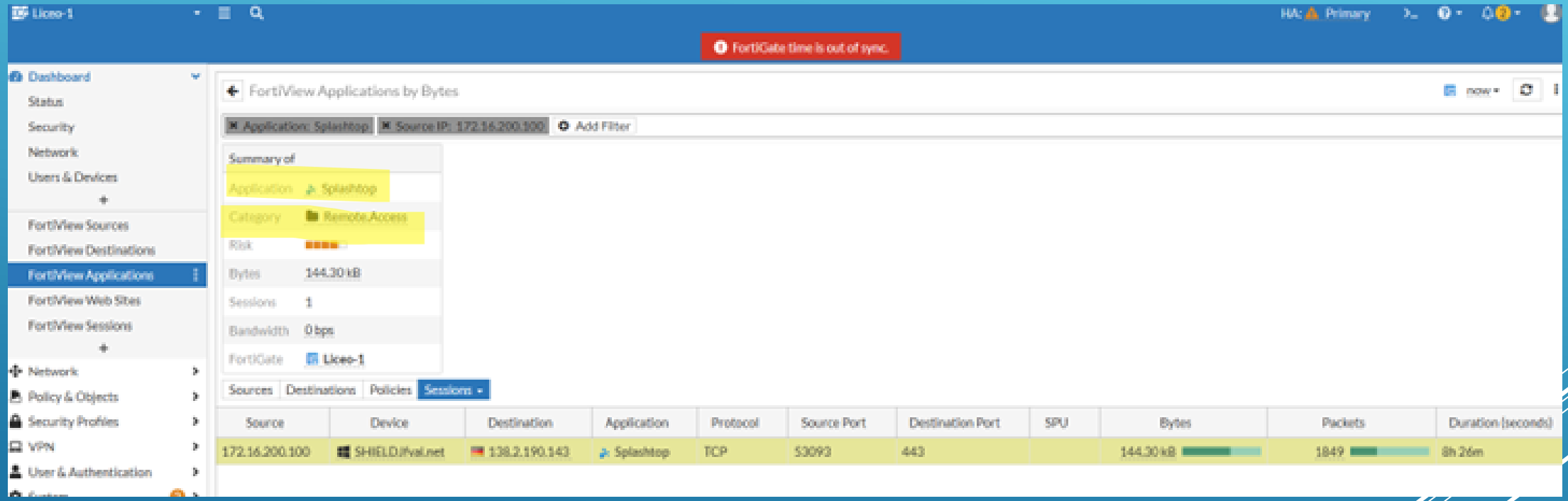
Se detecta aplicación de control remoto en los host de virtualización que se encuentran encriptados.





ANALISIS DEL CIBERATAQUE

Se detecta conexión establecida por dicha aplicación .



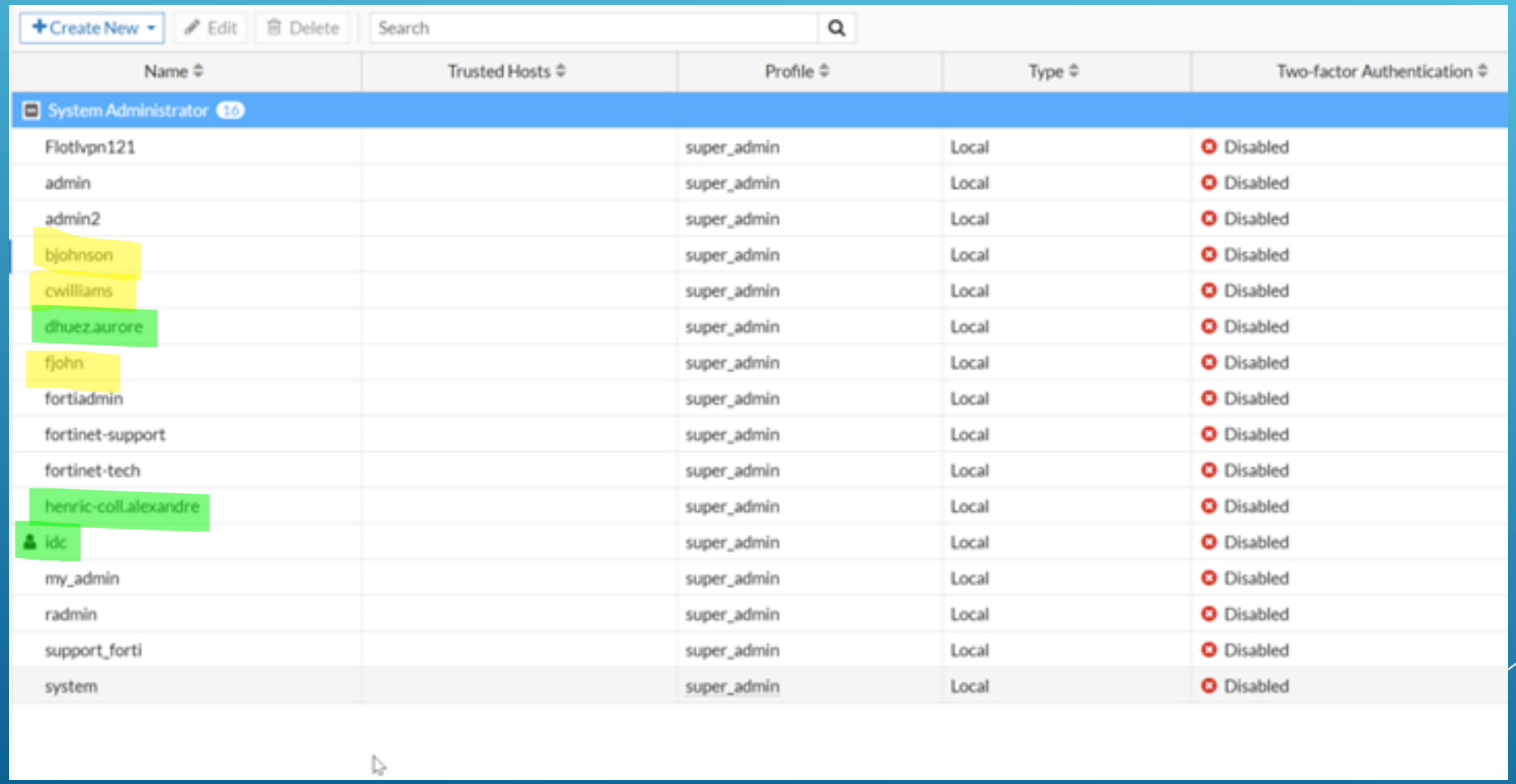
ANALISIS DEL CIBERATAQUE

Se detectan intentos de acceso a la administración del firewall desde fuera de la red local, debido a que las interfaces WAN tienen habilitada el servicio de gestión HTTPS.

Thursday		motorolasol...	Administrator motorolasolutions login failed from https(87.12...	Admin login failed
Thursday		tpgrefinance	Administrator tpgrefinance login failed from https(92.119.197....	Admin login failed
Thursday		admin	Administrator admin login failed from https(92.255.85.45) bec...	Admin login failed
Thursday			session clash	Session clashed
Thursday		hinghamsavi...	Administrator hinghamsavings login failed from https(92.119.1...	Admin login failed
Thursday			DHCP server sends a DHCPACK	DHCP Ack log
Thursday			DHCP server sends a DHCPACK	DHCP Ack log
Thursday			session clash	Session clashed
Thursday		westwaterr...	Administrator westwaterresources login failed from https(87....	Admin login failed
Thursday		admin	Administrator admin login failed from https(92.255.57.86) bec...	Admin login failed
Thursday		alarm	Administrator alarm login failed from https(92.119.197.11) be...	Admin login failed
Thursday			session clash	Session clashed
Thursday			DHCP server sends a DHCPACK	DHCP Ack log
Thursday		admin	Administrator admin login failed from https(92.255.85.174) be...	Admin login failed
Thursday			DHCP server sends a DHCPACK	DHCP Ack log
Thursday		dncadmin	Administrator dncadmin login failed from https(92.255.85.46) ...	Admin login failed
Thursday		ayagoldsilver	Administrator ayagoldsilver login failed from https(87.120.126...	Admin login failed

ANALISIS DEL CIBERATAQUE

Se detecta una anomalía en la cantidad de usuarios administradores del firewall. Únicamente deberían existir los usuarios administradores controlados.

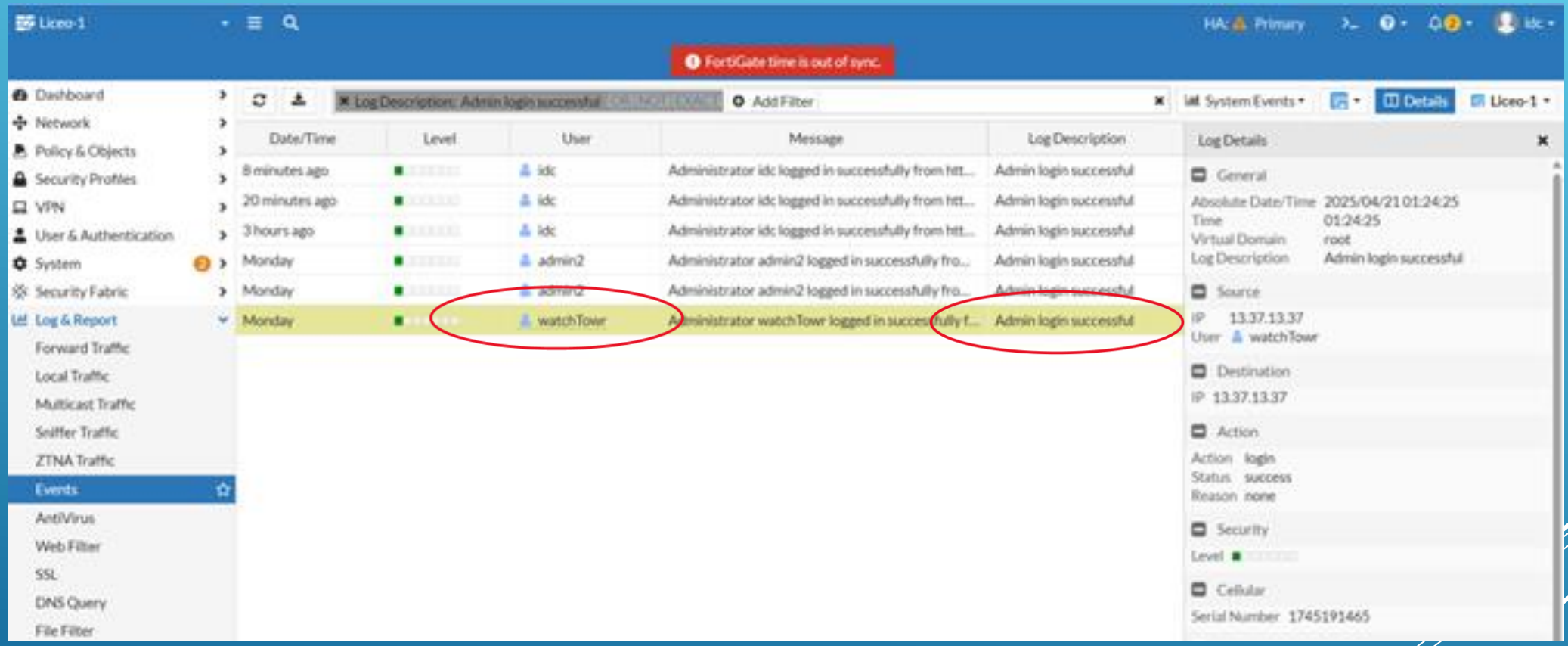


+ Create New | Edit | Delete | Search

Name	Trusted Hosts	Profile	Type	Two-factor Authentication
System Administrator 16				
Flotlvpn121		super_admin	Local	Disabled
admin		super_admin	Local	Disabled
admin2		super_admin	Local	Disabled
bjohnson		super_admin	Local	Disabled
cwilliams		super_admin	Local	Disabled
dhuez.aurore		super_admin	Local	Disabled
fjohn		super_admin	Local	Disabled
fortiadmin		super_admin	Local	Disabled
fortinet-support		super_admin	Local	Disabled
fortinet-tech		super_admin	Local	Disabled
henric-coll.alexandre		super_admin	Local	Disabled
idc		super_admin	Local	Disabled
my_admin		super_admin	Local	Disabled
radmin		super_admin	Local	Disabled
support_forti		super_admin	Local	Disabled
system		super_admin	Local	Disabled

ANALISIS DEL CIBERATAQUE

Finalmente se detecta un acceso no autorizado a la administración del firewall FortiGate



A partir de aquí se desencadenan una serie de eventos:

ANALISIS DEL CIBERATAQUE

Monday		admin	Administrator admin login failed from https(185.39.19.52) bec...	Admin login failed
Monday		watchTowr	Edit system.admin admin2	Object attribute configured
Monday		watchTowr	Administrator watchTowr logged in successfully from jsconsole	Admin login successful
Monday		admin2	Edit system.admin admin2	Object attribute configured
Monday		admin2	Edit system.admin admin2	Object attribute configured
Monday		admin2	Administrator admin2 logged in successfully from https(45.76...	Admin login successful
Monday		wiehman	Administrator wiehman login failed from https(87.120.127.2) ...	Admin login failed
Monday		admin2	Edit system.admin admin2	Object attribute configured
Monday		admin2	Administrator admin2 logged in successfully from https(45.76...	Admin login successful
Monday		wiehman	Administrator wiehman login failed from https(87.120.127.2) ...	Admin login failed
Monday		uvinson	Administrator uvinson login failed from https(92.119.196.21) ...	Admin login failed
Monday			Performance statistics: average CPU: 2, memory: 27, concurre...	System performance statistics
Monday		admin2	Edit vpn.ssl.settings	Attribute configured
Monday		wsnow	Administrator wsnow login failed from https(87.120.126.16) b...	Admin login failed
Monday			DHCP server sends a DHCPACK	DHCP Ack log
Monday		admin2	Administrator admin2 logged in successfully from jsconsole	Admin login successful
Monday		admin2	Edit user.group Administration	Object attribute configured

Type event
Sub Type system

Source
IP 45.76.128.203
User admin2

Destination

Source
IP 45.76.128.203
User admin2

Destination

User admin2

Action
Action Edit

Absolute Date/Time 2025/04/21 02:29:31
Time 02:29:31
Virtual Domain root
Log Description Admin login successful

ANALISIS DEL CIBERATAQUE

Se detectan conexiones VPN no autorizadas

Tras la detección de una conexión VPN desde Rumanía se establece la relación con la encriptación de las máquinas virtuales y los host.
Al no tener registros almacenados en el firewall anteriores a 5 días no podemos saber si se ha realizado algún tipo de exfiltración de datos, y tampoco desde cuando se tiene acceso la red interna

RECONSTRUCCIÓN

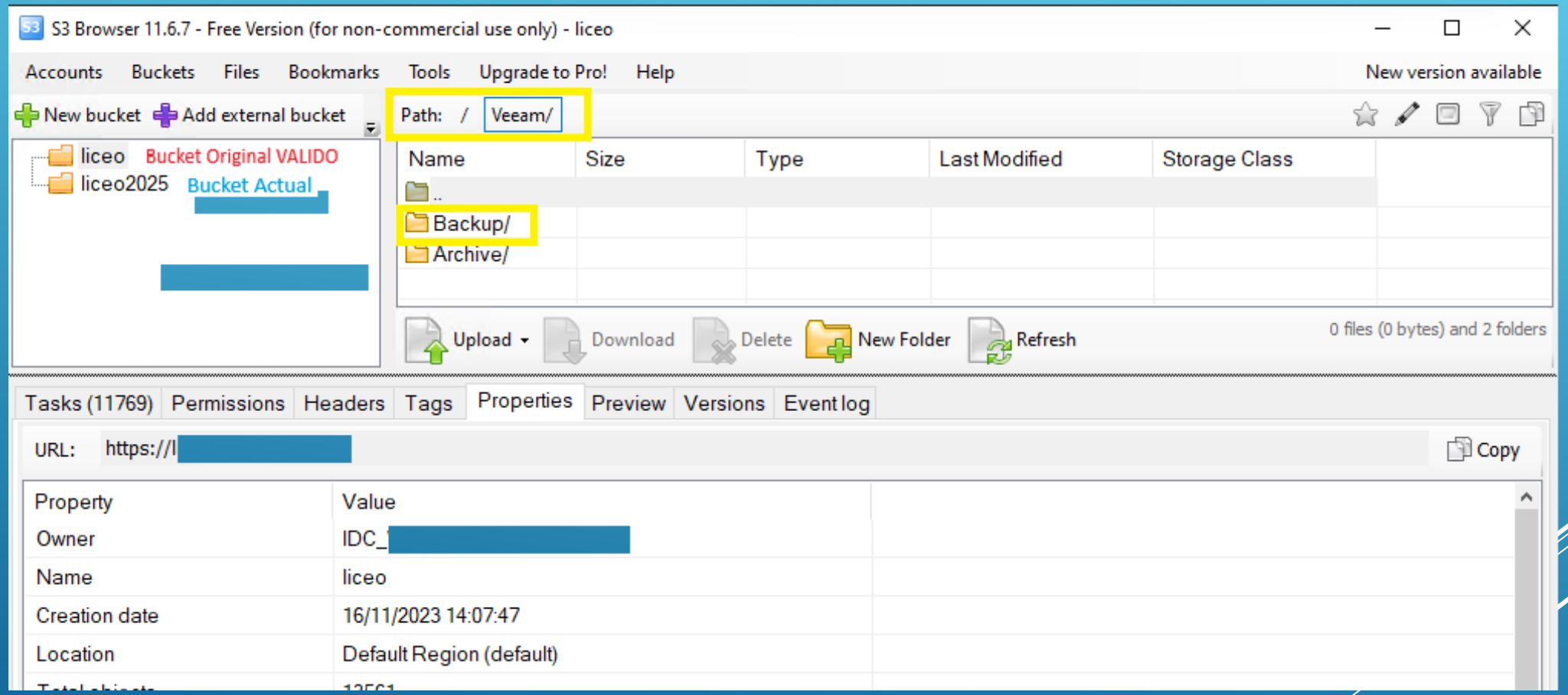
El equipo técnico de crisis designado empieza el protocolo de actuación reactivo frente a ciberataques:

- *Se revisa el alcance de dispositivos infectados* en cuanto a servidores y dispositivos cliente; se concluye de una AFECTACIÓN TOTAL en servidores, una afectación no concluyente en los dispositivos, El entorno de servidores se tiene que restaurar al completo.

- *Se revisa el plan de copias;* todas las copias locales se encuentran codificadas, las copias en el Datacenter de IDC parecen en correcto estado al ser inmunes.

RECONSTRUCCIÓN

La copia semanal lanzada al repositorio S3 al ser inmune no fue afectada:



HOJA DE RUTA

Se diseña una hoja de ruta para la puesta en producción del sistema:

- Apagado de uno de los dos cortafuegos deshaciendo la HA, limpieza del otro, aplicación de directivas restrictivas dejando que desde el exterior solo se pueda conectar la cuenta de IDC que es la única que dispone de doble factor de autenticación.
- Una vez asegurado el cortafuegos se genera un segmento limpio.
- Paralelamente se restauran los servidores necesarios desde el repositorio S3 externo en un sistema de virtualización que desplaza IDC a las instalaciones del Liceo recién instalado con el mismo hipervisor y con una maquina con el software de copias Veeam Backup conectado al repositorio S3.
- Este sistema se introduce en el segmento limpio, al igual que los clientes que se vayan validando.

Se da la fase de recuperación del sistema por acabada en este punto y se cierra como Fase 1 y se diseña la Fase 2 para devolver el sistema a su etapa original.

- Se formateará el segundo de los cortafuegos, se restaurará la alta disponibilidad y se parametrizará una configuración inicial.
- Se reconfigurarán los hosts de virtualización, la cabina de almacenamiento y el ecosistema de virtualización .
- Se devolverán las maquinas virtuales del sistema de IDC en el que residen al sistema original.
- Se revisará y acabará de configurar el sistema de una manera definitiva.

Se diseña una Fase3 de posible implementación que incluya las medidas proactivas y reactivas necesarias para intentar que la situación acaecida, en la medida de lo posible, no se repita.

PREVENCIÓN

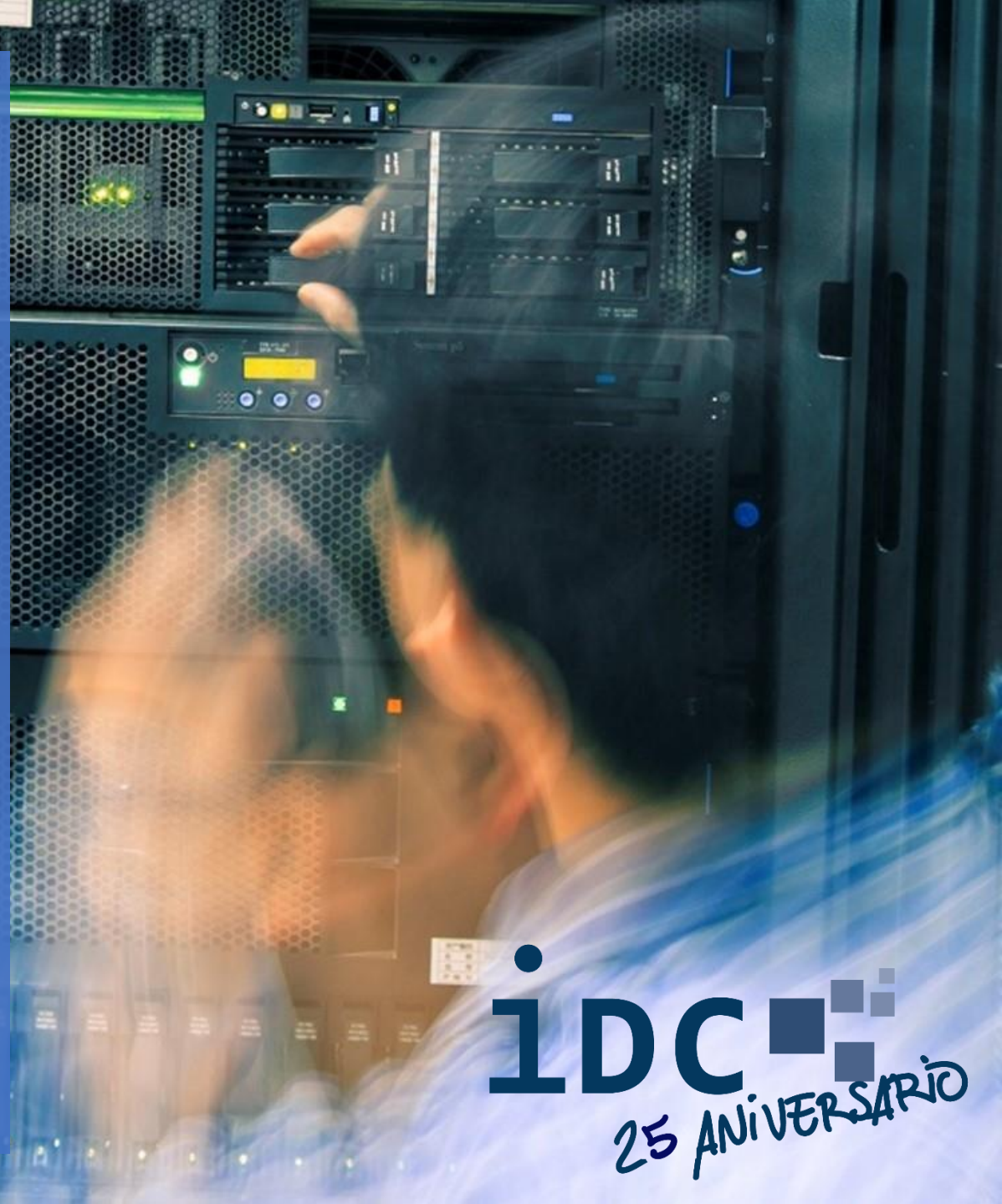
Fase 3; medidas:

- Mantenimiento premium de los cortafuegos, Incluye:
  - Actualizaciones y mantenimiento del cortafuegos.
  - Creación y almacenamiento de logs.
- Doble factor de autenticación.
- SOC.
- Segmentación.
- EDR/XDR/MDR

Microsoft

Gracias

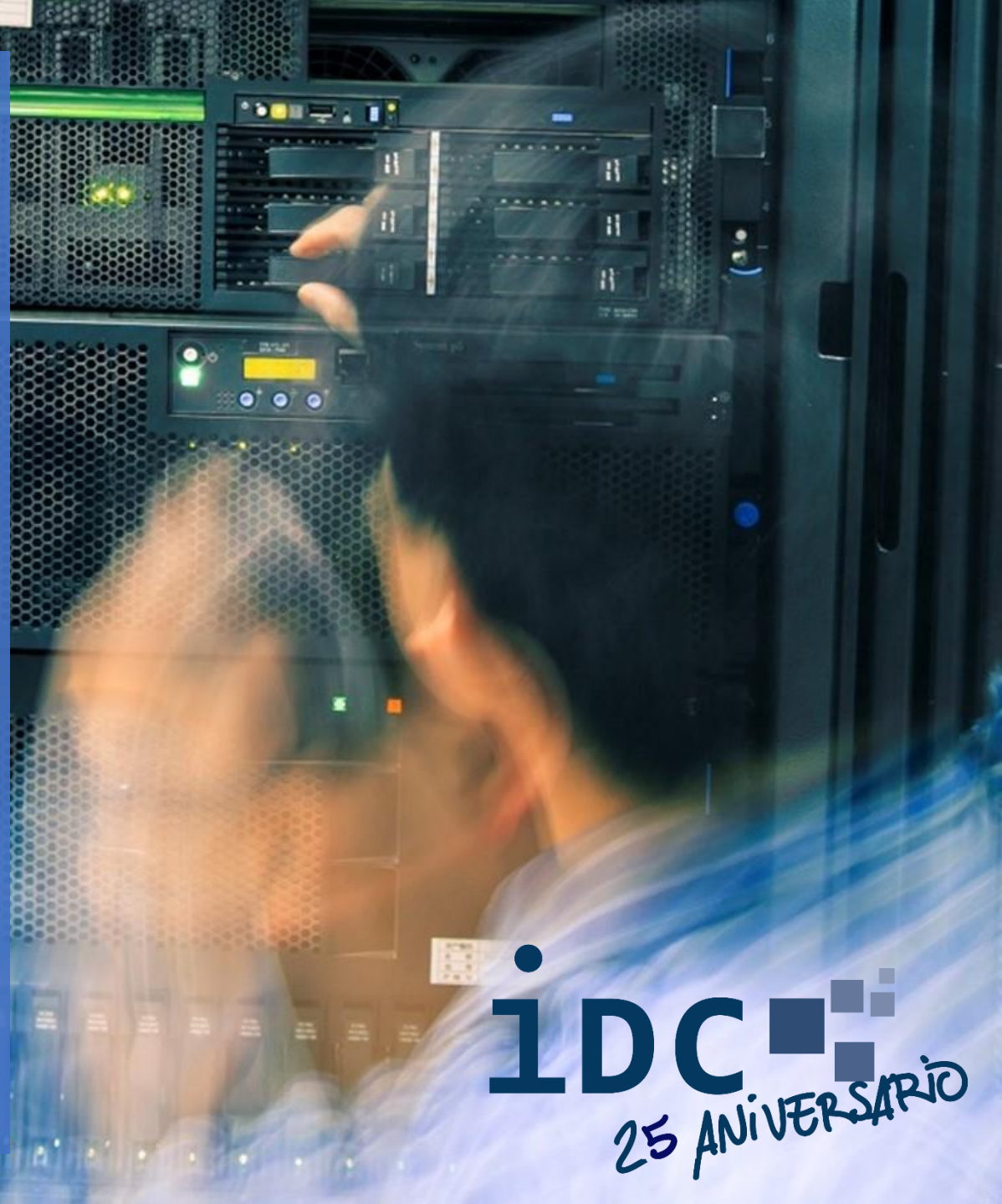
FORTINET



IDC 25 ANIVERSARIO

Microsoft

Pausa/café



Microsoft

Novedades a destacar

Cecilio Rodríguez
Director Comercial de IDC
Microsoft Certified System Engineer
CompTiA Server+ Certified
Microsoft Certified Associate

IDC 25 ANIVERSARIO

CICLO DE VIDA DEL SOFTWARE

El fin de vida de MS Windows 10 es en 2025, la actualización a MS Windows 11 es gratuita

Importante

Windows 10 llegará al fin de soporte el 14 de octubre de 2025. La versión actual, 22H2, será la versión final de Windows 10 y todas las ediciones seguirán siendo compatibles con las versiones de actualización de seguridad mensuales hasta esa fecha. Las versiones de LTSC existentes seguirán recibiendo actualizaciones más allá de esa fecha en función de sus ciclos de vida específicos.

Las fechas de soporte técnico se muestran en la zona horaria del Pacífico: Redmond, Washington (Estados Unidos).

Fechas de soporte técnico

Expandir tabla

Lista	Fecha de inicio	Fecha de retirada
Windows 10 Home y Pro	29 jul 2015	14 oct 2025

CICLO DE VIDA DEL SOFTWARE

El fin de vida de MS Windows 10 es en 2025, la actualización a MS Windows 11 es gratuita

Lista	Fecha de inicio	Fecha de retirada
Windows 11 Home y Pro	4 oct 2021	En soporte técnico

Versiones

Expandir tabla

Versión	Fecha de inicio	Fecha de finalización
Version 24H2	1 oct 2024	13 oct 2026
Version 23H2	31 oct 2023	11 nov 2025

CICLO DE VIDA DEL SOFTWARE

Productos que finalizan soporte en 2025

Access 2016	14 de octubre de 2025
Access 2019	
Dynamics 365 Business Central local (Directiva fija)	
Excel 2016	
Excel 2019	
Exchange Server 2016	
Exchange Server 2019	
Microsoft Office 2016	
Microsoft Office 2019	
Microsoft Report Viewer 2015 Runtime	
OneNote 2016	
Outlook 2016	
Outlook 2019	
PowerPoint 2016	
PowerPoint 2019	
Project 2016	
Project 2019	
Publisher 2016	
Publisher 2019	
Skype Empresarial 2016	
Skype Empresarial 2019	
Skype Empresarial Server 2015	
Skype Empresarial Server 2019	
Visio 2016	
Visio 2019	
Visual Studio 2015	
Visual Studio Team Foundation Server 2015	
Windows 10 2015 LTSB	
Windows 10 IoT Enterprise LTSB 2015	
Windows 10 Team (Surface Hub)	
Windows Defender Exploit Guard	
Windows Defender para Windows 10	
Windows Server 2012, actualización de seguridad extendida del año 2	
Windows Server 2012 R2, actualización de seguridad extendida del año 2	
Word 2016	
Word 2019	

LTSC es una versión de software de Microsoft que se centra en la estabilidad y la seguridad a largo plazo, ideal para entornos donde no se necesitan actualizaciones frecuentes y se prioriza la confiabilidad y la seguridad.

ADQUISICION DE VMware POR BROADCOM

Microsoft

¿Cómo nos afecta el cambio de licenciamiento de los productos VMware por parte de Broadcom?

- Eliminación de licencias perpetuas:
  - VMware, anteriormente, permitía a los usuarios adquirir una licencia única para usar el software sin límite de tiempo. Broadcom, sin embargo, ha migrado a un modelo de suscripción, que requiere una renovación anual, trianual o quinquenal
- Introducción de suscripciones:
  - Las licencias de VMware ahora se basan en suscripciones, que pueden ser anuales, trianuales o quinquenales. Estos paquetes incluyen funcionalidades agrupadas, lo que puede resultar en un aumento de costos para algunos usuarios.

IDC 25 ANIVERSARIO

ADQUISICION DE VMware POR BROADCOM

Microsoft

¿Cómo nos afecta el cambio de licenciamiento de los productos VMware por parte de Broadcom?

- Aumento de precios y pedido mínimo:
  - Broadcom ha impuesto un mínimo de 72 núcleos por pedido y por producto, lo que afecta especialmente a las pequeñas y medianas corporaciones, además de aumentar los precios.
- Cambios en el programa de partners:
  - Broadcom ha realizado cambios en el programa de partners, generando incertidumbre sobre los requisitos y beneficios para los socios.

IDC 25 ANIVERSARIO

ADQUISICION DE VMware POR BROADCOM

Microsoft

¿Cómo nos afecta el cambio de licenciamiento de los productos VMware por parte de Broadcom?

- Simplificación de la oferta:
  - Broadcom ha simplificado la cartera de productos de VMware, eliminando algunos productos independientes como Horizon, NSX, HCX, y vSphere+, o el ESXi gratuito.
- Despidos:
  - Se han producido despidos en la plantilla de VMware, lo que ha reducido la fuerza laboral de la empresa a casi la mitad, (de 38.000 trabajadores en 2023 a 16.000 en la actualidad), y se espera que Broadcom continue con la reducción de personal.

IDC 25 ANIVERSARIO

ADQUISICION DE VMware POR BROADCOM

Microsoft

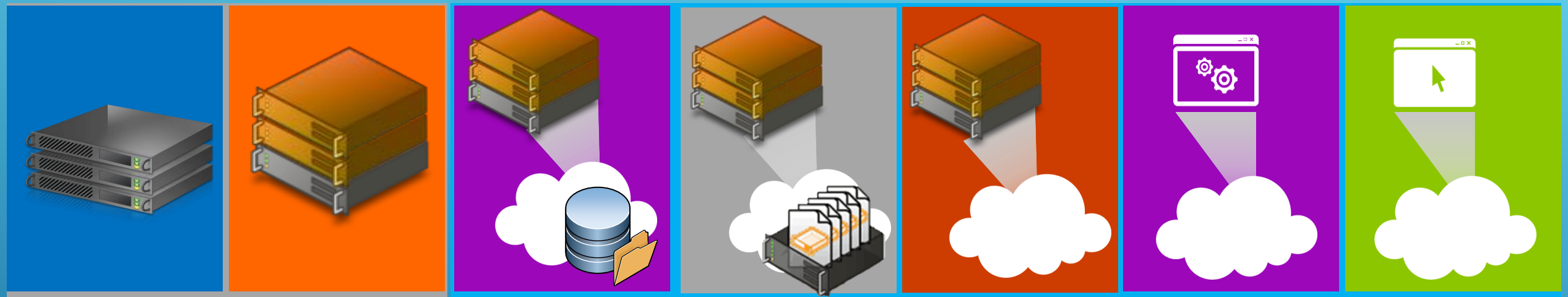
¿Soluciones?

- Pagar:
  - Seguir una estrategia continuista, adaptarnos a las nuevas exigencias, y continuar con el producto a la espera de que sean todos los cambios a corto plazo, los realizados.
- Cambiar el hipervisor:
  - Migrar a un hipervisor que cumpla con los estándares necesarios y cuyo coste sea asumible, (Proxmox, Hyper-V).
- Migrar a IaaS/PaaS:
  - Migrar nuestro sistema a un Datacenter externo con lo cual el hipervisor es transparente para nosotros.

IDC 25 ANIVERSARIO

VISIÓN ESTRATÉGICA DE IDC EN LAS AALL

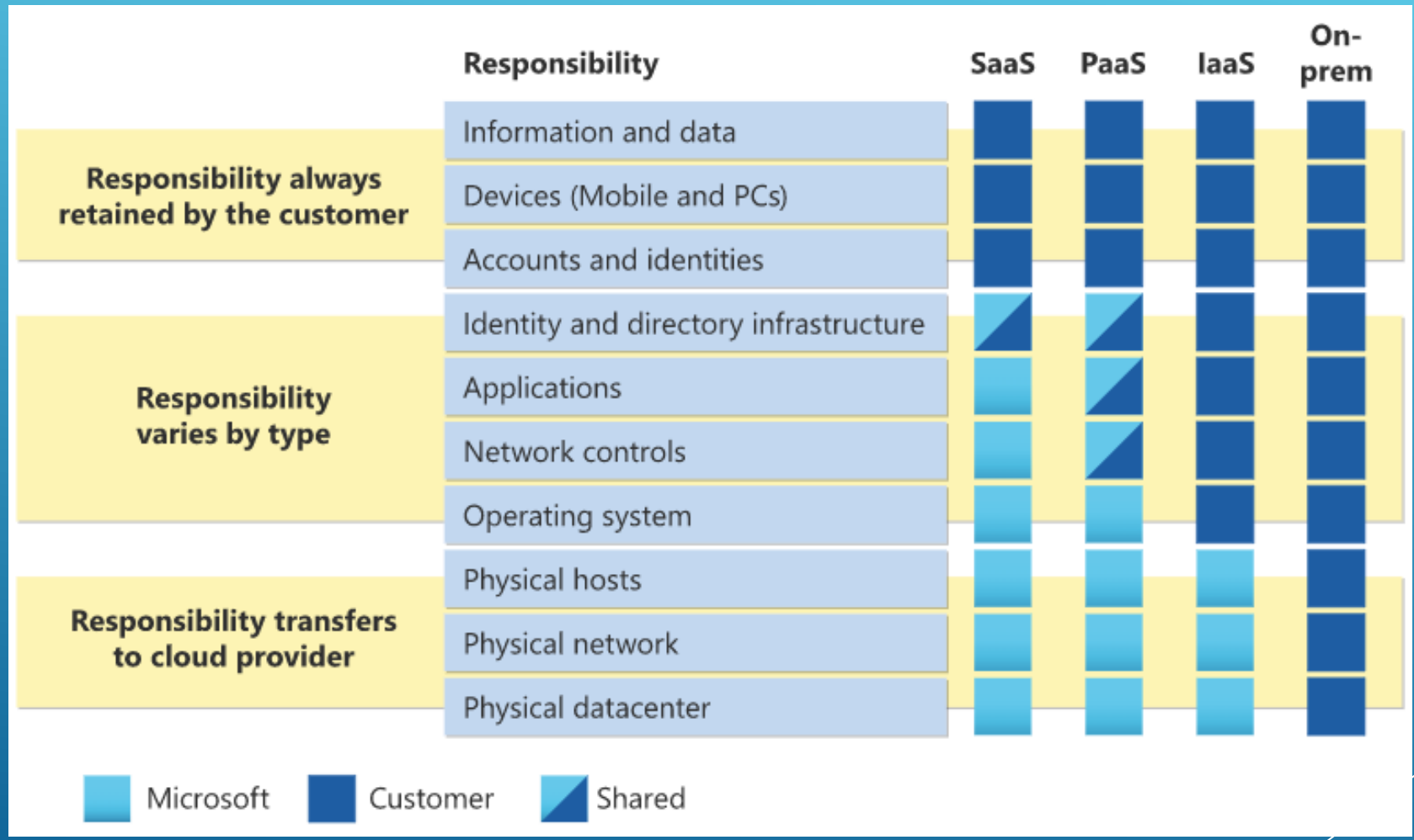
SaaS como objetivo, globalización del servicio como servicio.



VISIÓN ESTRATÉGICA DE IDC EN LAS AALL

Microsoft

SaaS como objetivo, globalización del servicio como servicio.

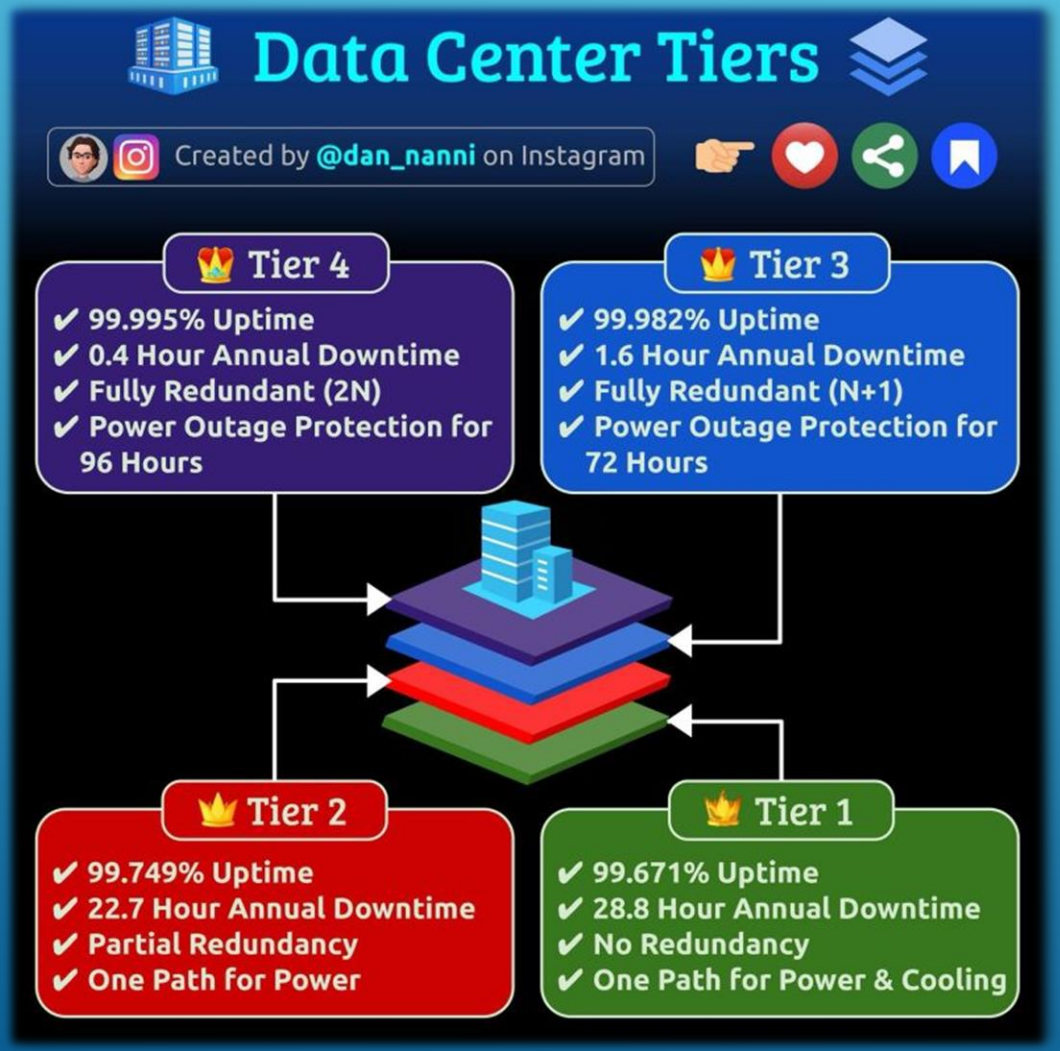


IDC 25 ANIVERSARIO

IDC Cloud

IDC 25 ANIVERSARIO

Categorías de clasificación de los Datacenter



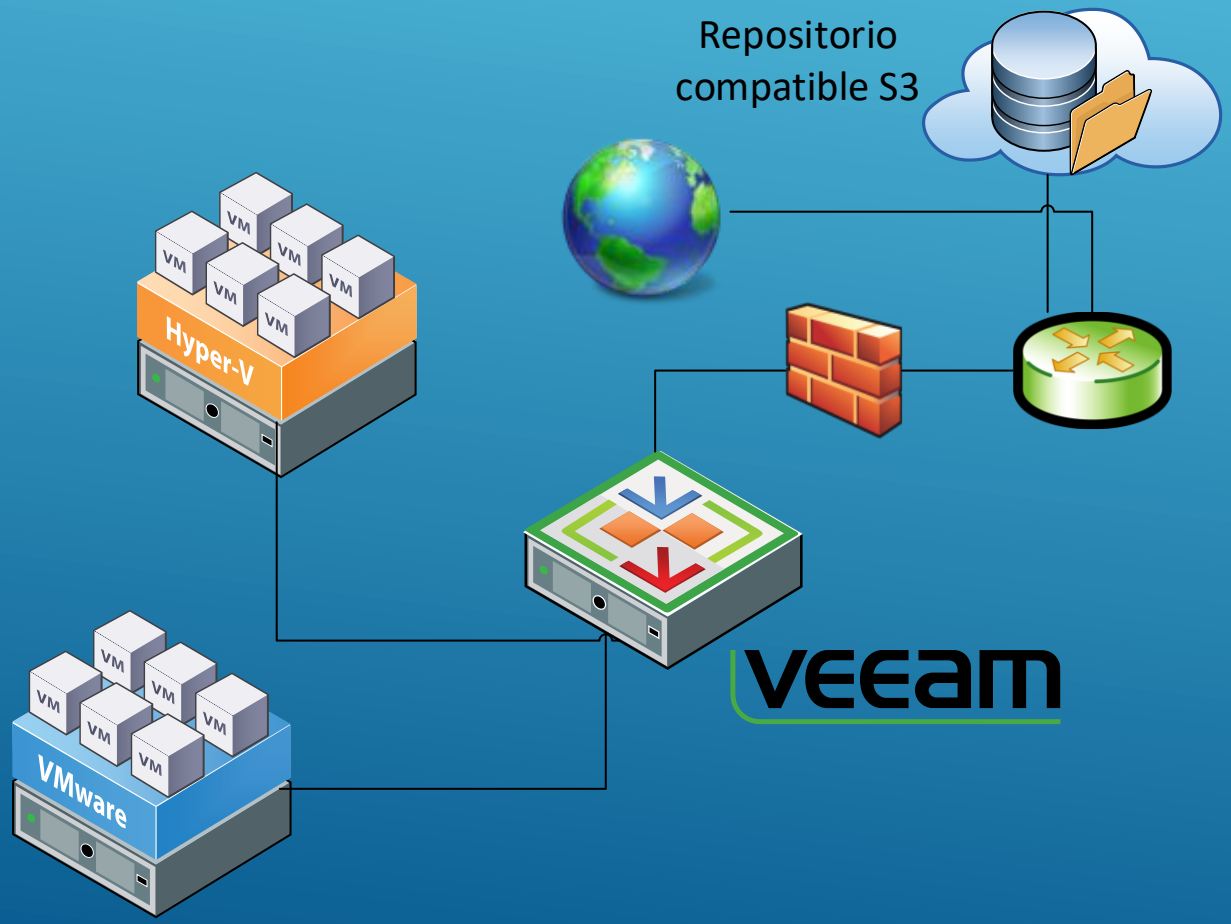
IDC 25 ANIVERSARIO

IDC Cloud ofrece los siguientes servicios:

- BaaS: Backup como servicio.
- RaaS: Replica de maquinas virtuales como servicio.
- IaaS: Infraestructura como servicio.
- Paas: Plataforma como servicio.

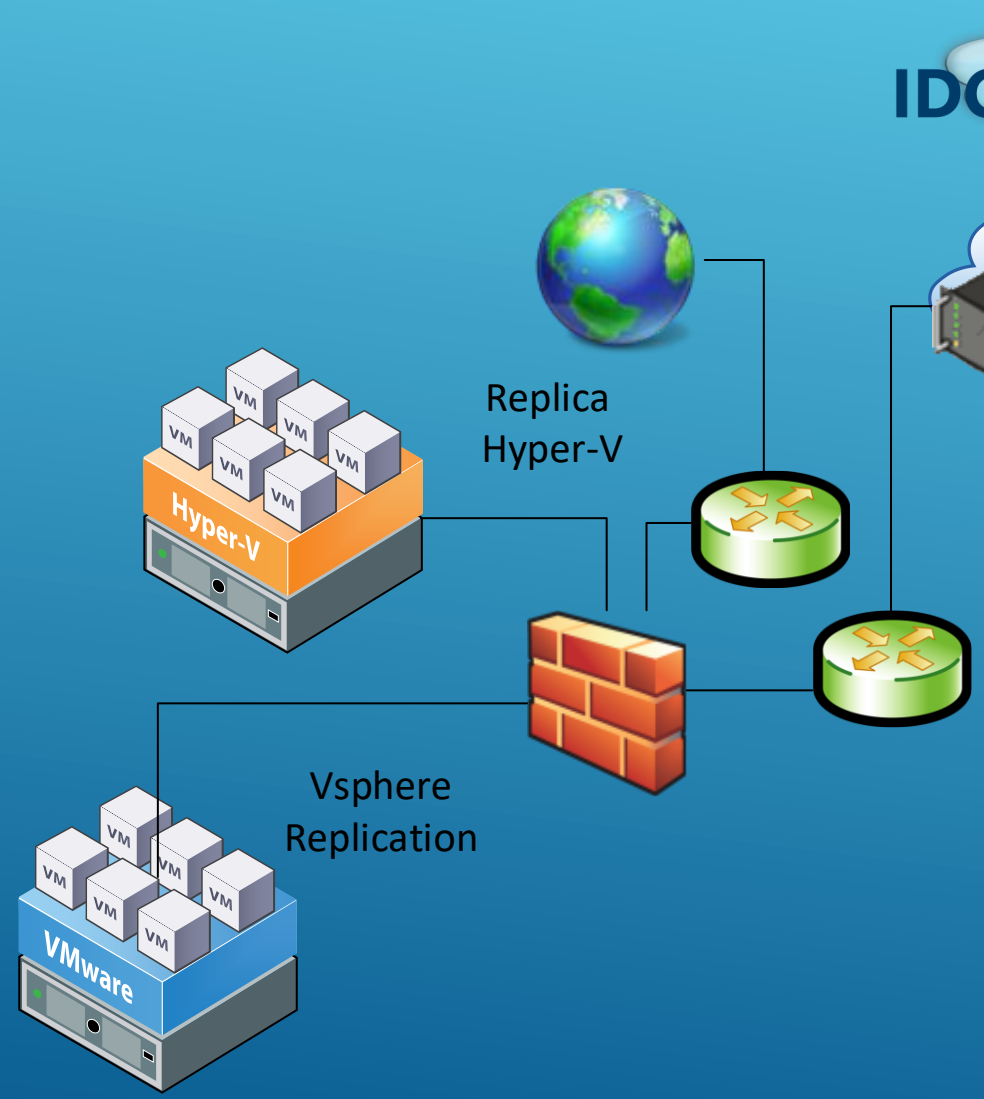
IDC Cloud

BaaS



- Pago por uso → 15€/TB de ocupación al mes, precio final.

RaaS



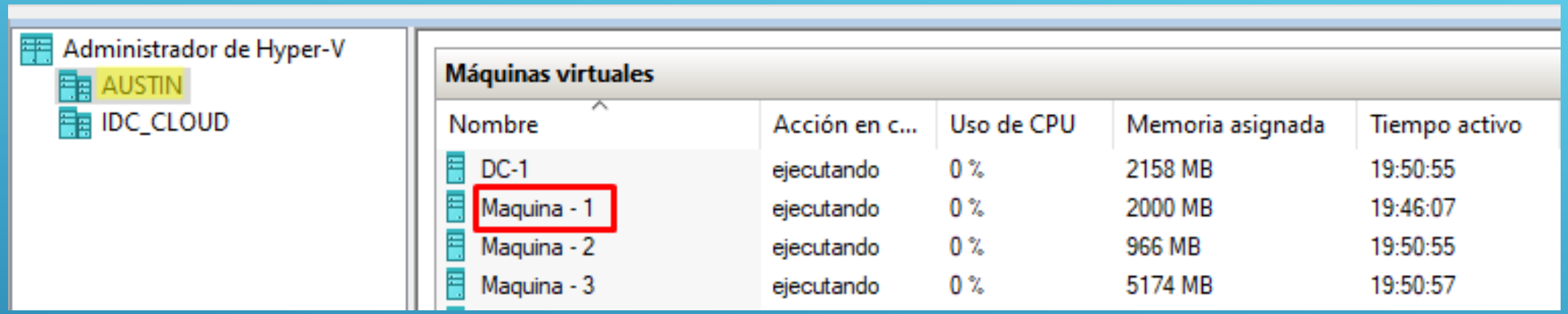
- Ejemplo con 15 máquinas + 3,5TB
  - Circuito de 600Mps → 150€
  - Nº Maquinas virtuales → 15 x 5€/Ud.
  - Espacio ocupado → 4 x 50€/TB
  - Total =150+75+ 200= 425€/mes
  - Reserva de recursos → 10% = 47,5€/mes

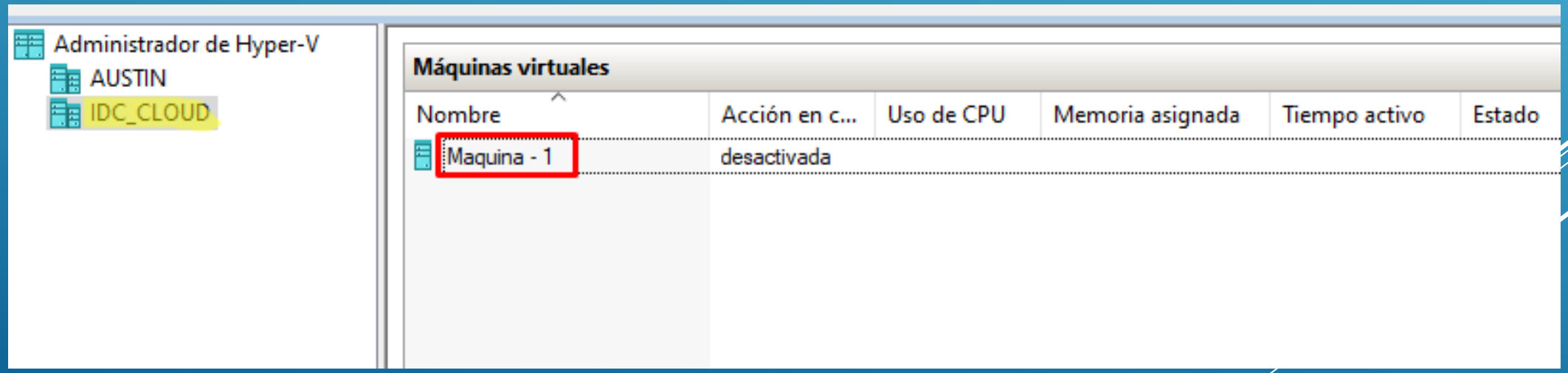
- Pago por uso
  - Circuito de 600Mps → 150€
  - Nº Maquinas virtuales → 5€/Ud.
  - Espacio ocupado → 50€/TB
  - Reserva de recursos → 10%

IDC Cloud

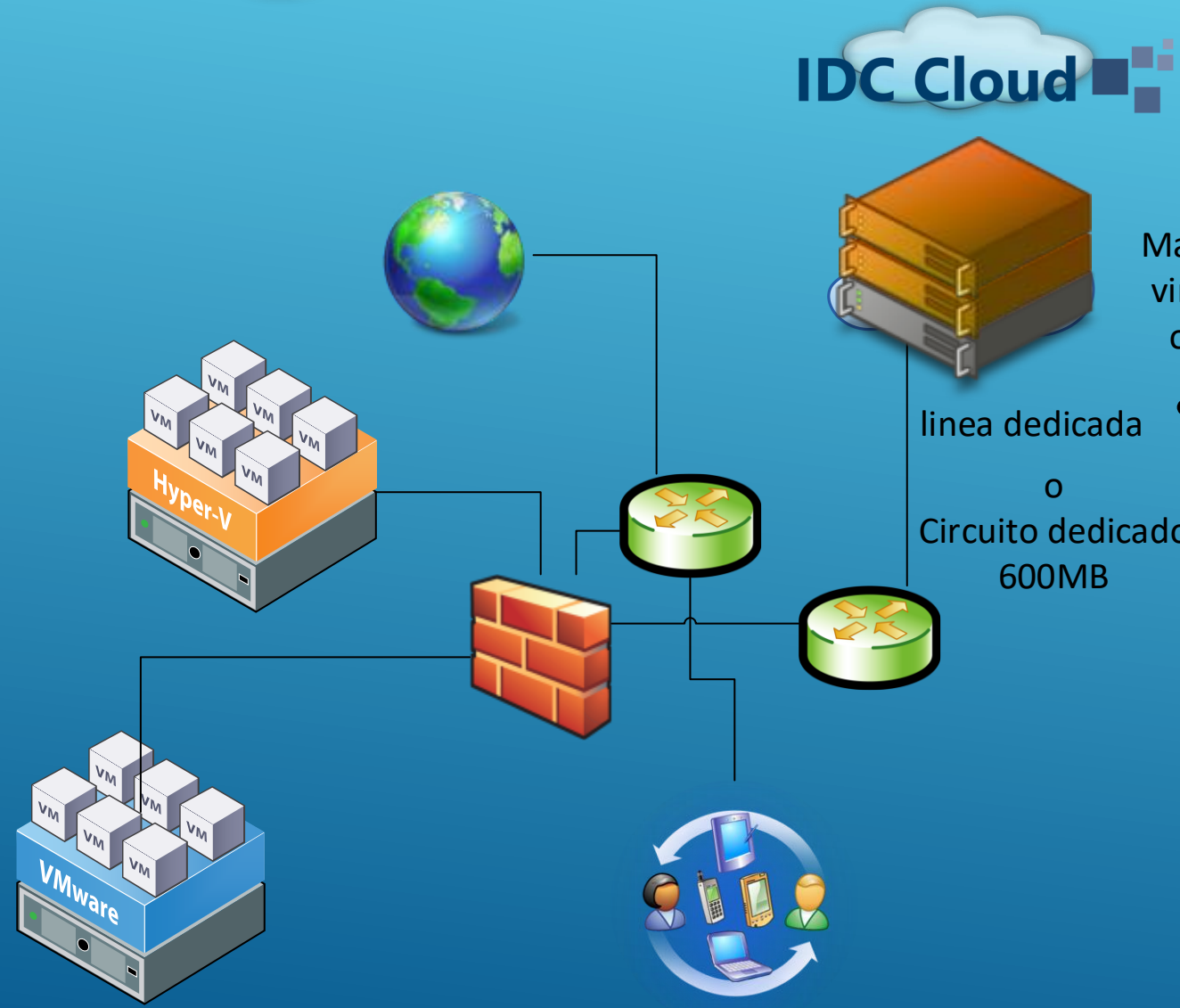
RaaS

IDC 25 ANIVERSARIO





IaaS/PaaS



- Pago por uso
  - Circuito de 600Mps → 150€
  - Opción de línea dedicada → Consultar
  - Maquinas virtuales por tipo desde 15€/Ud.
  - Posibilidad de configuración a medida o ampliaciones de las máquinas tipo
  - Espacio ocupado → 50€/TB

IDC Cloud

IaaS/PaaS

IDC 25 ANIVERSARIO

Demo.

¡¡¡Gracias!!!