Hewlett Packard Enterprise

CONTINUIDAD DE NEGOCIO PARA UNA NUEVA ERA

Felipe López, Data Protection Manager, HPE Latin America

Marzo 2022

UNA NUEVA ERA PARA LA PROTECCIÓN DE DATOS

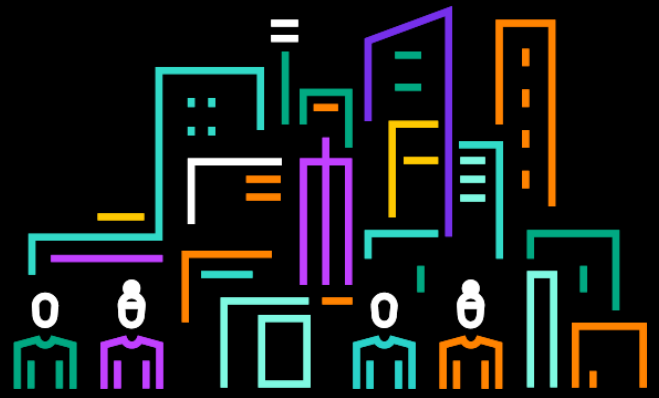
Los datos impulsan su estrategia de transformación digital

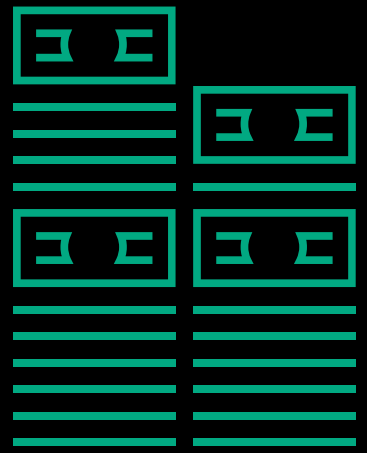
Necesitan estar siempre protegidos y seguros

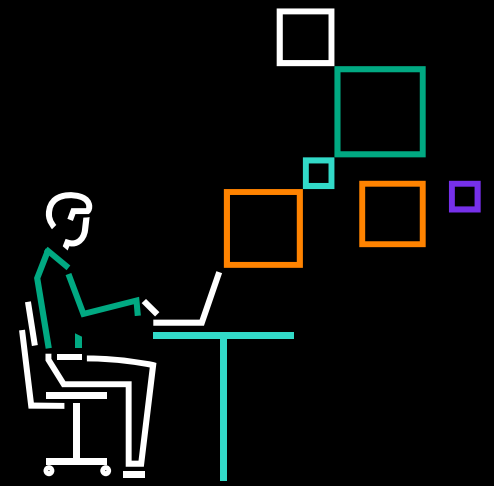
Y disponibles al instante, donde y cuando sea necesario

En un mundo siempre conectado, el tiempo de inactividad y la pérdida de datos pueden resultar catastróficos

EL COSTO Y EL RIESGO DE LA PERDIDA DE LOS DATOS: CATASTRÓFICO







73%[1]

de las empresas requirieron acceso ininterrumpido

$20M[1]

es reportado por las empresas como pérdida anual de tiempo de inactividad

54%[1]

de las empresas afirmaron haber perdido la confianza del cliente debido a interrupciones

[1]*2019 Veeam Cloud Data Management Report*

LA PROTECCIÓN DE DATOS ES CADA VEZ MÁS DESAFIANTE

- El crecimiento de los datos se está acelerando
- La expansión de la copia de datos secundarios está aumentando
- Los requisitos de SLA se están transformando
- El panorama de las amenazas y el cumplimiento está evolucionando
- La TI híbrida está creando complejidad

EXPLOSIÓN DE DATOS

ESTAMOS ENTRANDO EN LA ERA DE ZETTABYTE

Crecimiento explosivo desde el borde hasta la nube

1 **Zettabyte** (ZB)
= 1000 Exabytes
= 1 millón de petabytes
= 1000 millones de terabytes

[1]*Source: IDC Data Age 2025 sponsored by Seagate, 2018*

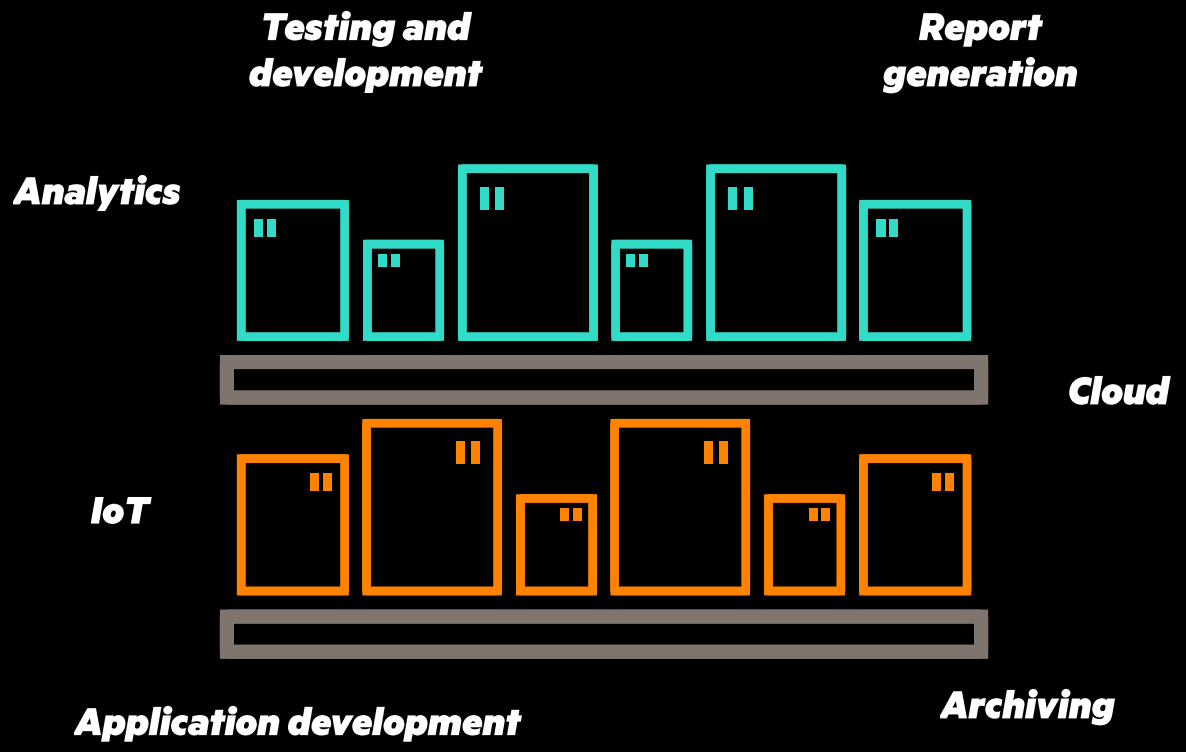
EL CRECIMIENTO DE DATOS REPRESENTA TAMBIÉN UNA EXPANSIÓN DE COPIAS DE SEGURIDAD

Este crecimiento representa un importante gasto en infraestructura de almacenamiento

Del 40 % al 50 % de los datos se dedica a las copias[1]

El 82% de las empresas tienen al menos 10 copias de cualquier instancia de datos.[1]

Las organizaciones asignan el 56 % de su segunda capacidad de almacenamiento a actividades de gestión de datos[2]



1 *"IDC Market Glance: Copy Data Management, 2Q18"*
2 *"ESG Master Survey Results: Copy Data Management Trends," March 2018*

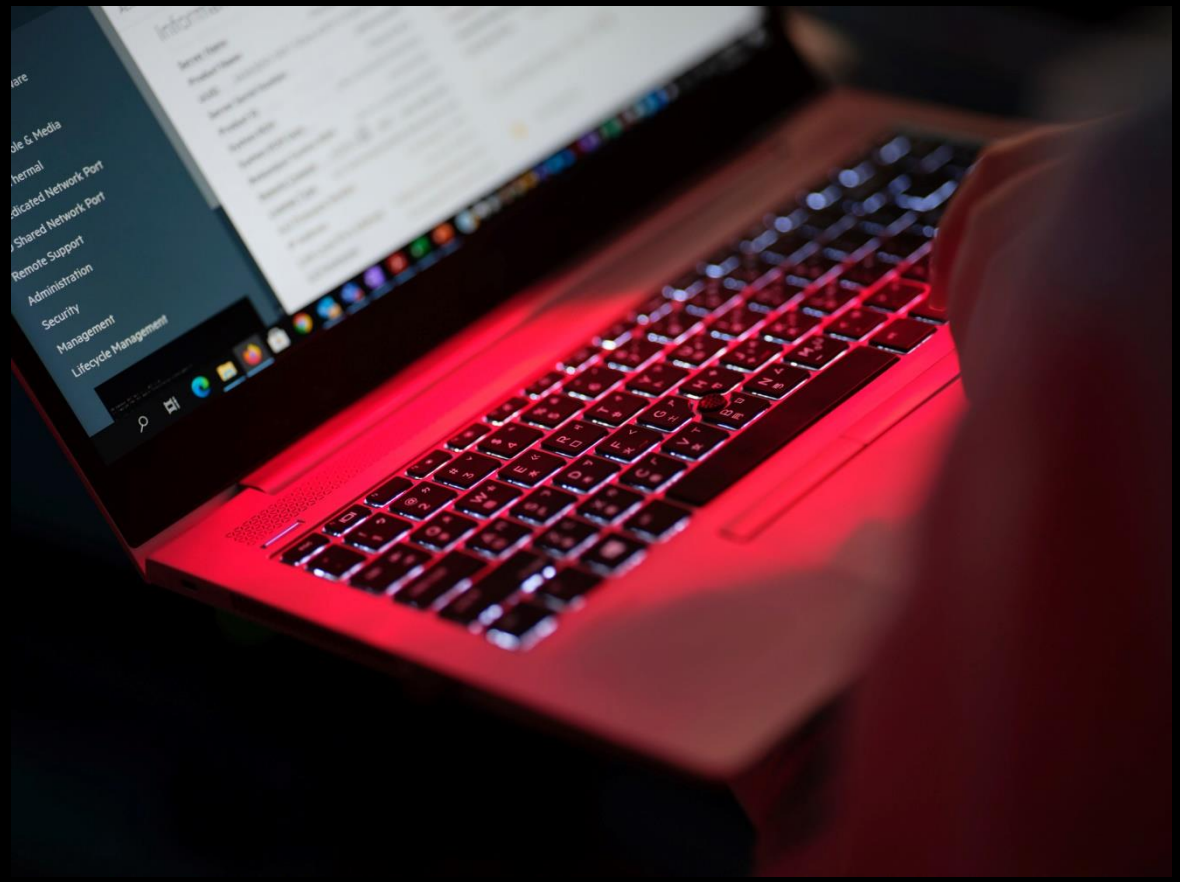
RANSOMWARE

63%

De las organizaciones encuestadas han sido objetivo de ataques de **ransomware en los últimos 12 meses**

Source: ESG Custom research commissioned by HPE, November 2021

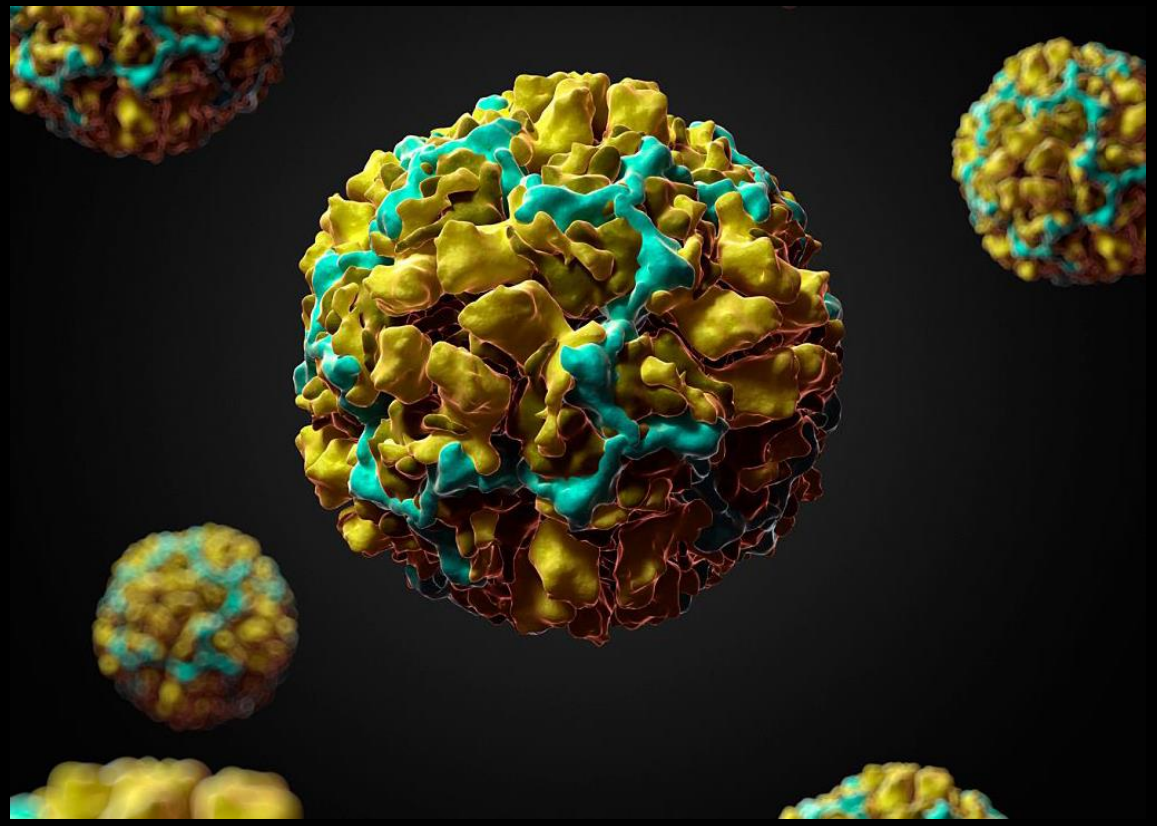
¿QUÉ ES RANSOMWARE?



- Un tipo de software maligno (o malware) que previene a los usuarios acceder a su información, con el propósito de Extorsión
- **Ransom** del inglés, que significa “rescate”:
- El Ransomware encripta la información y sus respaldos, amenazando con borrar los datos o hacerlos públicos, a menos que se pague un rescate.

¿DE DONDE VIENE EL RANSOMWARE?

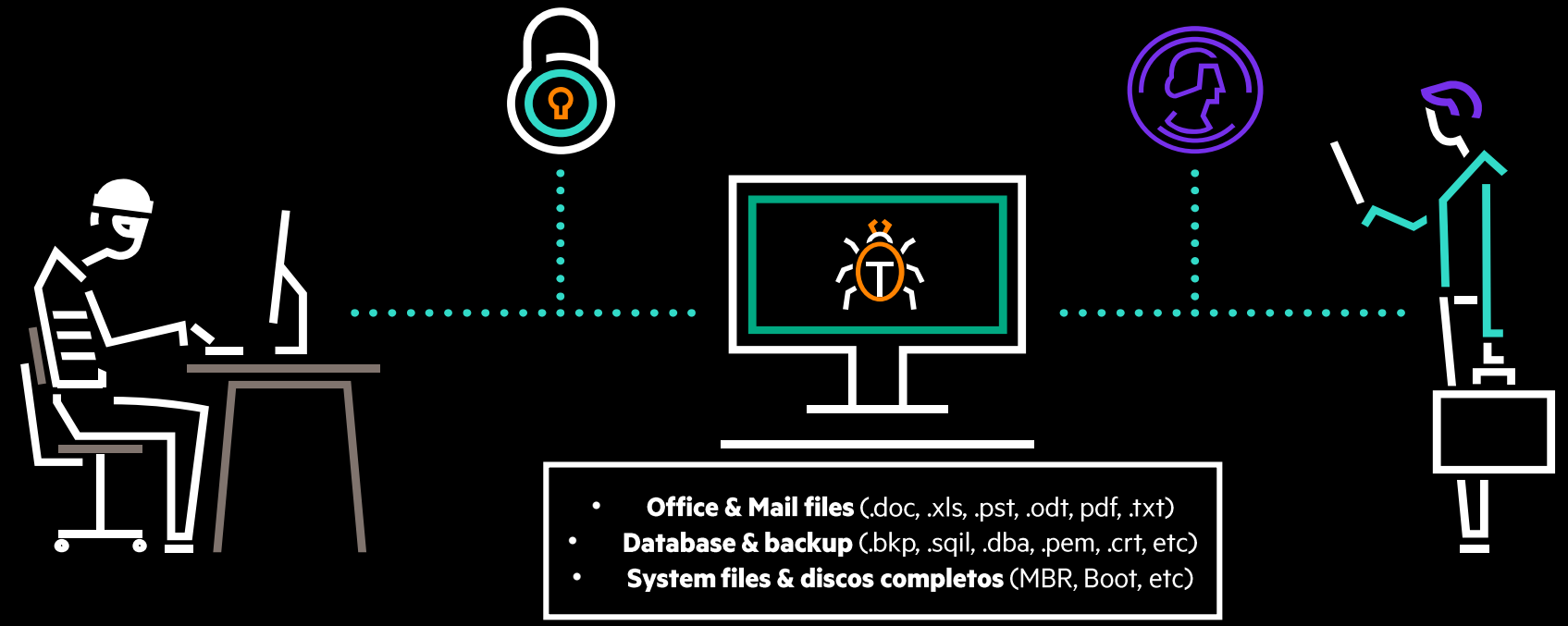
El nacimiento del **BitCoin** en 2008 y su apertura como software de código abierto en 2009, el crecimiento exponencial del uso de **la crypto-moneda** hizo aún más atractivo para los **cyber-delicuentes** el programar nuevos **virus** enfocados a obtener pagos de rescates con pagos digitales, más difíciles de rastrear.



El primer gran ataque de **ransomwware**, sucedió en 2013 conocido como **Cryptolocker**, esparcido a través de correo electrónico, demandando **$400 en Bitcoin** en un plazo máximo de 72 horas. ½ millón de infectados, 1.3% pagaron el rescate, con un estimado de pagos por $27 Millones de dólares

- https://time.com/nextadvisor/investing/cryptocurrency/what-is-bitcoin/#:~:text=Bitcoin%20was%20created%20in%202009,value%20currency%2C%20comparable%20to%20gold.
- https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

¿CÓMO ACTÚA EL RANSOMWARE?



- **Office & Mail files** (.doc, .xls, .pst, .odt, pdf, .txt)
- **Database & backup** (.bkp, .sqil, .dba, .pem, .crt, etc)
- **System files & discos completos** (MBR, Boot, etc)

ATAQUE CYBERNÉTICO

El Ransomware entra por *phishing* o aprovechando alguna vulnerabilidad en seguridad del Sistema Operativo, logrando visibilidad de sus archivos y en especial, busca los repositiorios de respaldo visibles en la red por el Sistema operativo

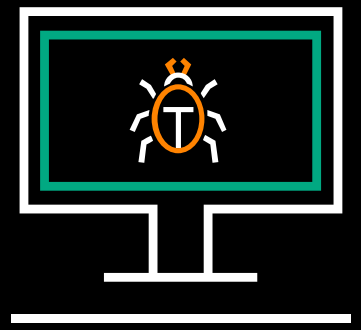
INFECCIÓN DEL SISTEMA

El Ransomware procede a encryptar la información almacenanada en el centro de datos, equipo portatil o cuenta hackeada: las copias primarias y secundarias (backup) son también encriptadas, para que la recuperación no sea algo sencillo.

DEMANDA DE PAGO

El Ransomware presenta un mensaje en pantalla o envía un mensaje/correo electrónico altertando a la víctima de la situación, el monto a pagar con cryptomoneda, y el plazo para entregar la llave de encripción y recuperar el acceso

¿QUÉ HACER FRENTE AL ATAQUE DE RANSOMWARE?



¿Mi sistema fue infectado?

NO

SI

¿Tengo Respaldos disponibles? (Backup/DR)

SI

NO

Recuperar la información y continuar la operación

Pagar o Perder la información (o Pagar y Perder los datos)

¿Qué tan rápido me puedo recuperar?

¿Qué tanta información perdí consecuencia del ataque?

Para mitigar un ataque de **ransomware**, debo contar con una estrategia de **continuidad de negocio** a nivel de diversos componentes:

- Seguridad de la red
- Antivirus
- Tecnología de Servidores y Almacenamiento
- Tecnología de Respaldo
- **Estrategia de respaldo y recuperación**

MODERNIZAR LA PROTECCIÓN DE DATOS: ESENCIAL PARA TODA EMPRESA

51%	Consideran la mejora de la seguridad y la protección de los datos como la prioridad No. 1 [1]
91%	de las Organizaciones Industriales son Vulnerables a los Ciberataques[2]
50%	Las organizaciones han sufrido una pérdida de datos irrecuperable[3]

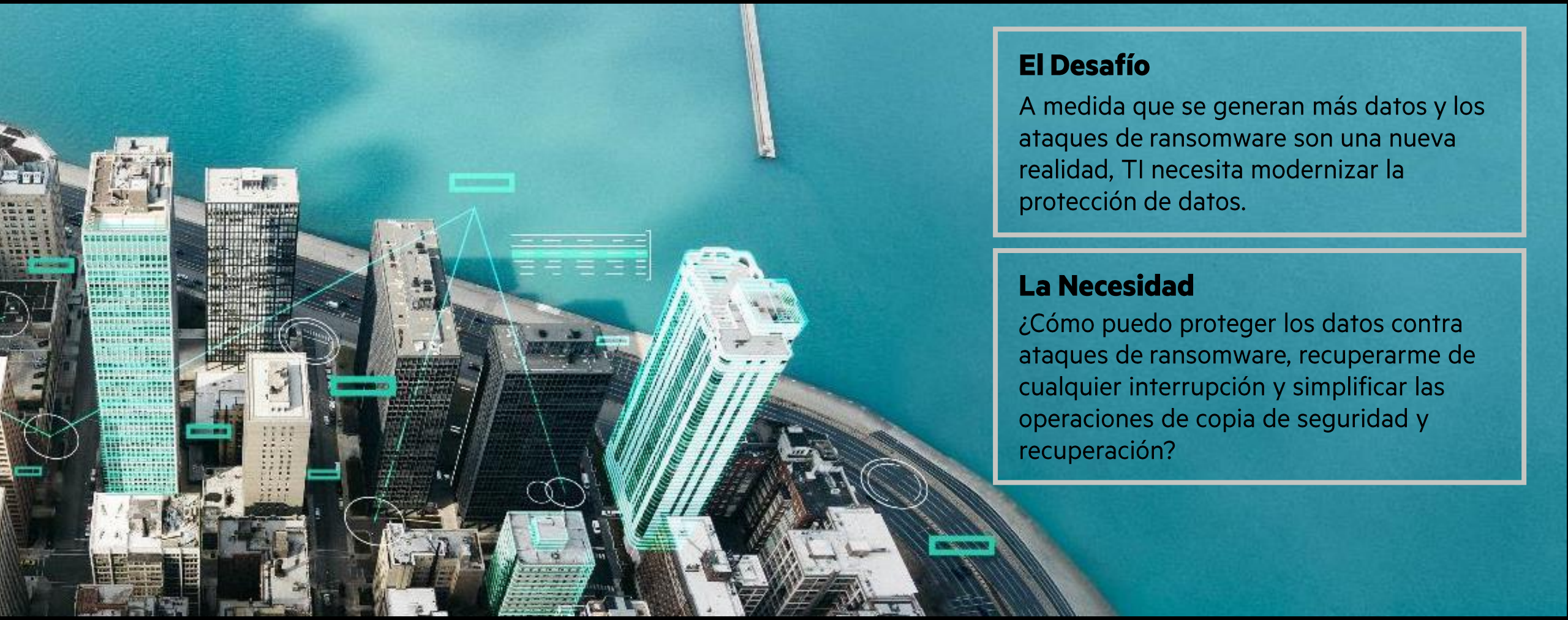
1. ESG Market Research of IT Decision Makers, April 2021
2. Information security risks report, September 2021
3. Data Protection for Hybrid Cloud, Containers, and Virtual Machines, IDC Infobyte

PROTECCIÓN DE DATOS PARA LA NUEVA ERA

- Data Protection
- 3-2-1-1

LOS DATOS SON EL MOTOR DE SU ORGANIZACIÓN

Crecimiento explosivo desde el borde hasta la nube



El Desafío

A medida que se generan más datos y los ataques de ransomware son una nueva realidad, TI necesita modernizar la protección de datos.

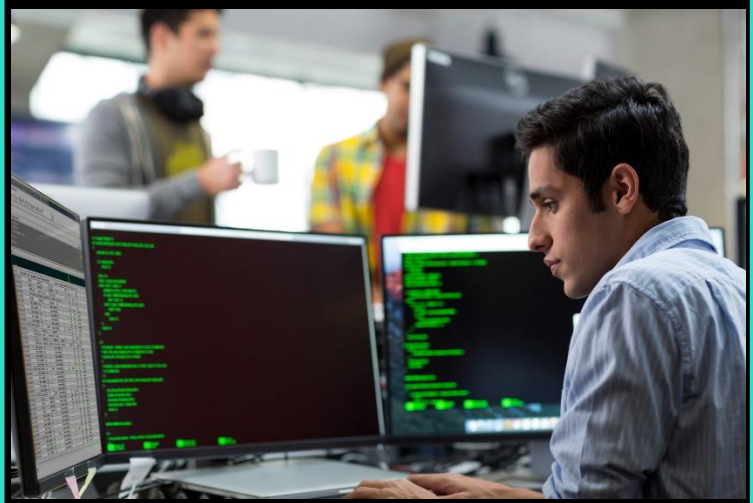
La Necesidad

¿Cómo puedo proteger los datos contra ataques de ransomware, recuperarme de cualquier interrupción y simplificar las operaciones de copia de seguridad y recuperación?

CONTINUIDAD DE NEGOCIO: 3 PUNTOS CLAVE A IMPLEMENTAR

LA MEJOR PRÁCTICA EN PROTECCIÓN DE DATOS

Regla del 3-2-1-1



LA TECNOLOGÍA CORRECTA EN PROTECCIÓN DE DATOS

Mitigar que suceda un desastre

UNA ESTRATEGIA PARA RECUPERACIÓN DE DESASTRES

En caso que suceda un desastre

IMPLEMENTAR LA MEJOR PRÁCTICA: LA REGLA 3-2-1-1

Protección de datos contra CUALQUIER falla, dondequiera que viva

3 copias de datos, 2 copias, en 2 tipos de medios diferentes, 1 copia fuera del sitio, 1 fuera de línea

1ra Copia:

Almacenamiento Primario

2da Copia:

Dispositivo de copia de seguridad en disco

En las instalaciones

3ra Copia:

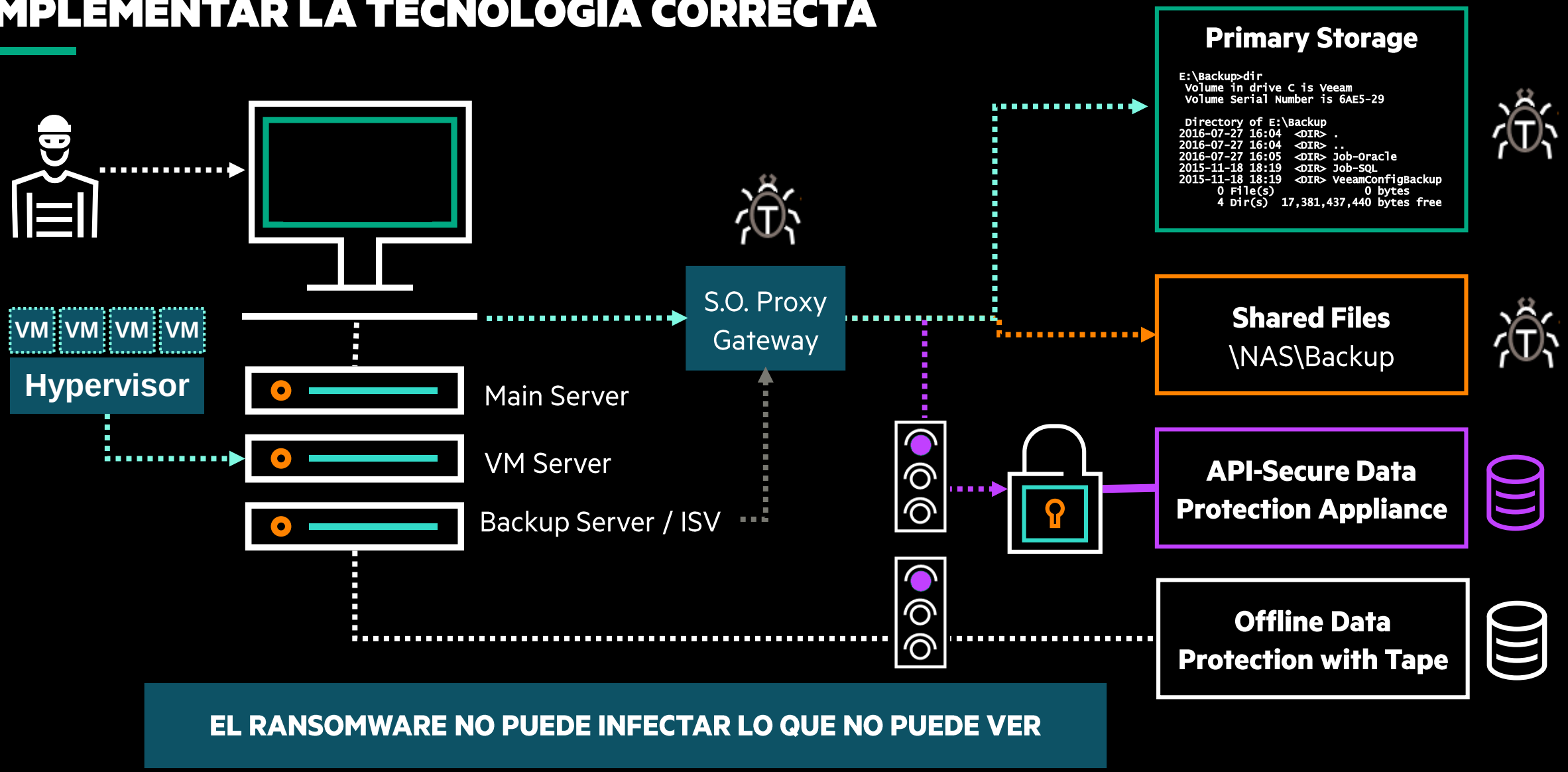
Dispositivo de copia de seguridad en disco

o copia de seguridad en la nube

y/o copia de seguridad en cinta

Fuera del sitio

IMPLEMENTAR LA TECNOLOGÍA CORRECTA



RECUPERACIÓN DE DESASTRES

- Disaster Recovery
- Edge-to-Cloud protection

MECANISMOS DE CONTINUIDAD DE NEGOCIO

Cuando se necesita la continuidad del negocio o la recuperación ante desastres, dicha acción generalmente implica el inicio de un conjunto de actividades y tecnologías para restablecer las operaciones de TI: a nivel de arquitectura; implica rápidamente poner en producción un sitio alterno.

- El primer paso generalmente implica llamar a un equipo de recuperación de desastres designado. Una vez que los responsables están en el trabajo, pueden promulgar los pasos necesarios para recuperarse siguiendo el plan de recuperación ante desastres de la organización.
- La continuidad del negocio es similar porque también está impulsada por un plan y se invoca cuando algún tipo de interrupción puede poner en peligro (pero no destruir) la infraestructura de TI de una organización.
- Un plan de continuidad del negocio describe de cómo mantener el negocio en funcionamiento cuando aparecen posibles interrupciones, algo que refiere a una infraestructura alternativa

¿Qué tan rápido me puedo recuperar?

¿Qué tanta información perdí consecuencia del ataque?

Métricas asociadas a la continuidad de negocio

- **RTO:** se refiere al período de tiempo que un sistema, servicio o aplicación puede no estar disponible o estar inactivo sin causar pérdidas o daños significativos a una empresa u organización.
- **RPO:** donde RTO mide el tiempo de inactividad máximo sostenible, RPO mide la pérdida de datos máxima sostenible. Por lo tanto, RPO a menudo se expresa como una medida de tiempo, desde el momento de la interrupción o pérdida hasta la copia de seguridad o instantánea anterior más reciente.

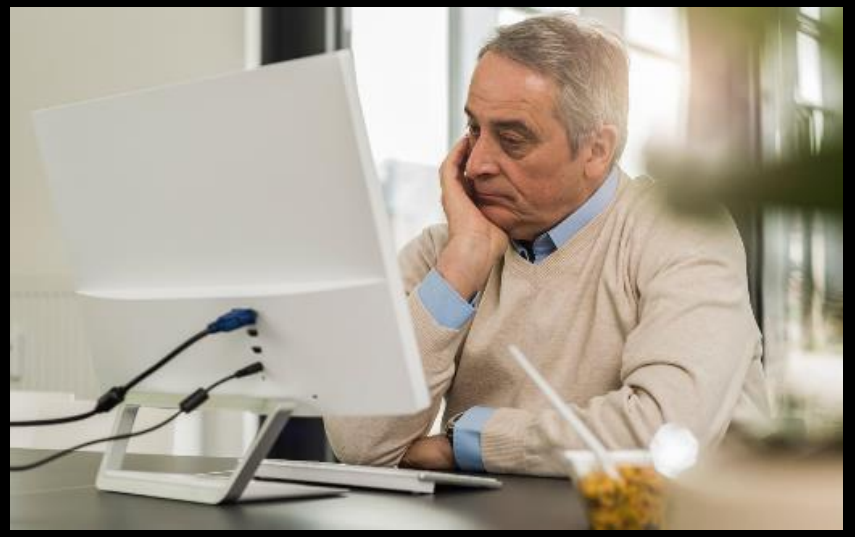
RECUPERACIÓN DE DESASTRES VS BACKUP

DISASTER RECOVERY

- Replicación al sitio secundario o recuperar en un sitio secundario
- Aplicaciones T1-2
- Bajo RPO/RTO
- Recuperación de ransomware
- Rendimiento optimizado
- Recuperación híbrida

Dos tipos de diseño diferentes

BACKUP



- Copia de seguridad en almacenamiento secundario
- Todas las aplicaciones
- RPO/RTO Promedio
- Recuperación de último recurso Costo optimizado Inmutable

OPTIMIZAR LA TECNOLOGÍA PARA LA CONTINUIDAD EN TODO ESCENARIO

RANSOMWARE RECOVERY

- Recuperación a escala
- Recuperar a segundos antes de un ataque
- Análisis forense de datos

DISASTER RECOVERY

- Fallas de hardware
- Desastres naturales
- Cortes de energía
- Pruebas automatizadas

BACKUP & RECOVERY

- Errores de usuario
- Eliminaciones de archivos
- Corrupciones

LONG-TERM RETENTION

- Requerimientos legales
- Recuperación de cumplimiento

MULTI-CLOUD MOBILITY

- Migraciones
- Híbrido, multinube
- Consolidaciones de centros de datos
- Modernización de Infraestructura

EL OBJETIVO: MODERNIZAR LA PROTECCIÓN DE DATOS Y ASEGURAR LA CONTINUIDAD DE NEGOCIO

Seguro contra Ransomware

Recuperación más rápida de un ataque de ransomware; encriptado de fin a fin; restauraciones granulares de ataques cibernéticos

Recuperarse de cualquier interrupción

RPO y RTO líderes en la industria; combinación correcta de DR, copia de seguridad; flexibilidad de restauraciones instantáneas y retención a largo plazo en la nube

Protección sin esfuerzo y sin pagar de más

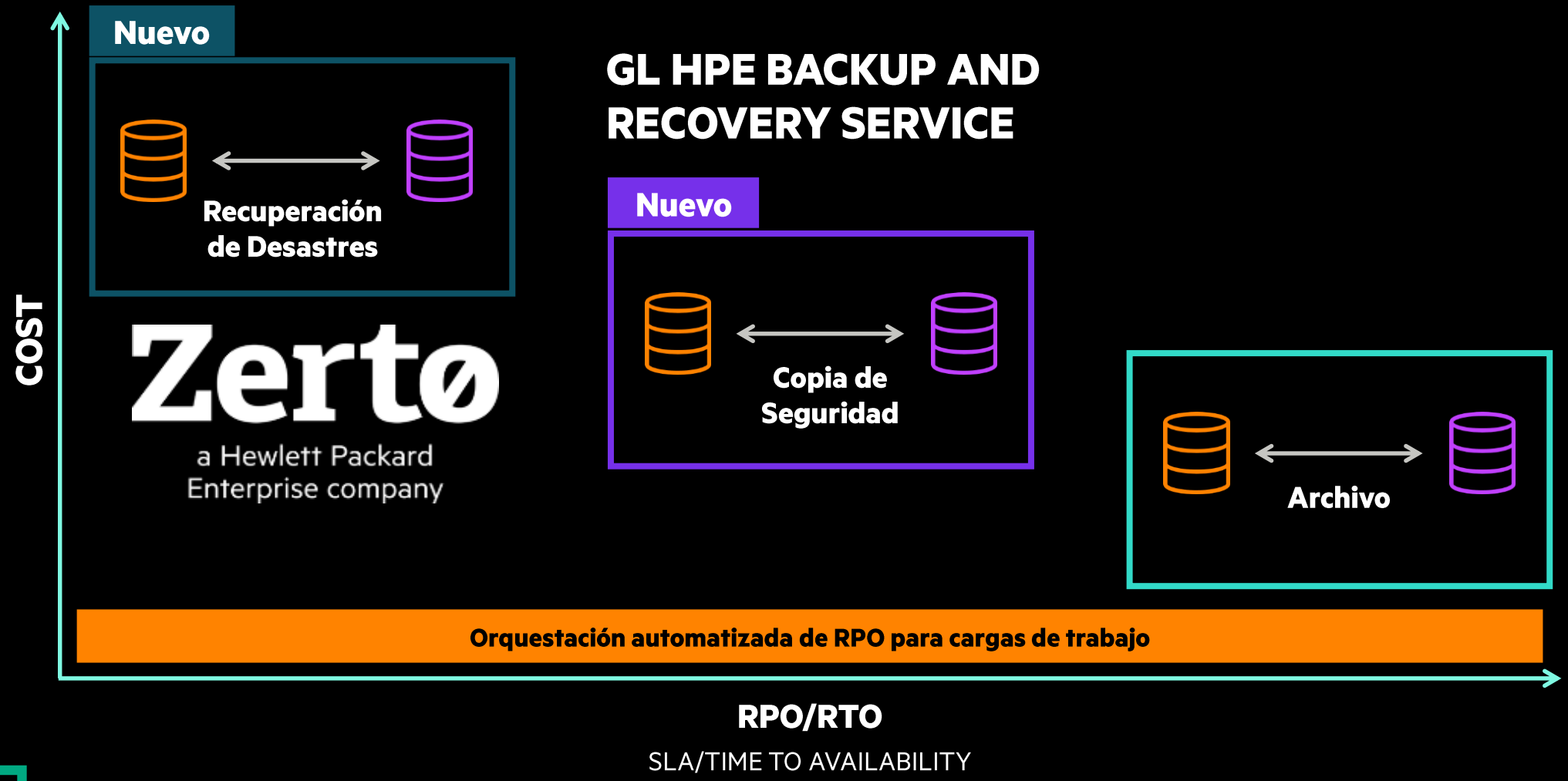
Automatización impulsada por políticas; borde de gestión unificado a la nube; entregado como un servicio

CONTINUIDAD DE NEGOCIO CON HPE

- HPE GreenLake for Data Protection
- HPE Data Protection & Recovery Solutions

HPE GREENLAKE FOR DATA PROTECTION

Modernización de la protección de datos del perímetro a la nube



HPE DATA PROTECTION & RECOVERY SOLUTIONS

Snapshots Integration

HPE Alletra

HPE Nimble Storage dHCI

HPE Primera & Nimble

Primary Backup

HPE DSCC: Backup and Recovery Service

HPE StoreOnce

HPE Apollo 4000

Backup Copy

Cloud Backup

HPE StoreOnce

HPE StoreEver

Long Term Retention

Cloud Archive

HPE StoreOnce

HPE StoreEver

Integration

- Veeam
- Commvault
- Cohesity
- Amazon
- Vmware
- Microsoft
- Scality
- Micro Focus
- Google
- etc

Zerto
a Hewlett Packard Enterprise company

HPE GreenLake as-a-service

Hewlett Packard
Enterprise

GRACIAS

Felipe López, Data Protection Manager, HPE Latin America

Marzo 2022