Superintendencia de Bancos de Panamá

XIX JORNADA DE ACTUALIZACIÓN BANCARIA 2021

"Los Retos de un marco regulatorio inclusivo en la Gestión Judicial"

Ana Verdegais
Regional Account Manager
North of Latin America
Data Protection Solutions
ana.verdegais@dell.com

Ciber Resilencia

Recuperándonos de un ataque cibernético

DELL Technologies

Si la información es el nuevo oro…
¡HAY QUE PROTEGERLA!

2020 marcó el inicio de lo que Dell Technologies llama la era de los datos.

Las empresas están basadas en datos, lo que los convierte en un activo muy valioso.

30 mil millones de registros de datos fueron robados en 2020, más que en los 15 años anteriores juntos.
(Canalys)

Las soluciones de ciberseguridad y privacidad se encuentran entre las primeras tres inversiones de TI.
(Índice de Transformación Digital de DT)

Las organizaciones están administrando

+ 10 VECES

la cantidad de datos que hace **CINCO AÑOS**

ElCapital
FINANCIERO.COM

ECONOMÍA | EMPRESAS | ACTUALIDAD | MIS FINANZAS | INTERNACIONALES | ESPECIALES

Panamá sufrió más de 1,8 billones de intentos de ciberataques

EN ECONOMÍA, TOP NEWS noviembre 19, 2019 Redacción

LA ESTRELLA DE PANAMÁ

Economía //

Panamá, entre los diez países con más ciberataques en Latinoamérica

'Phishing', la modalidad de ciberataque más frecuente en Panamá. **Shutterstock**

A nivel mundial

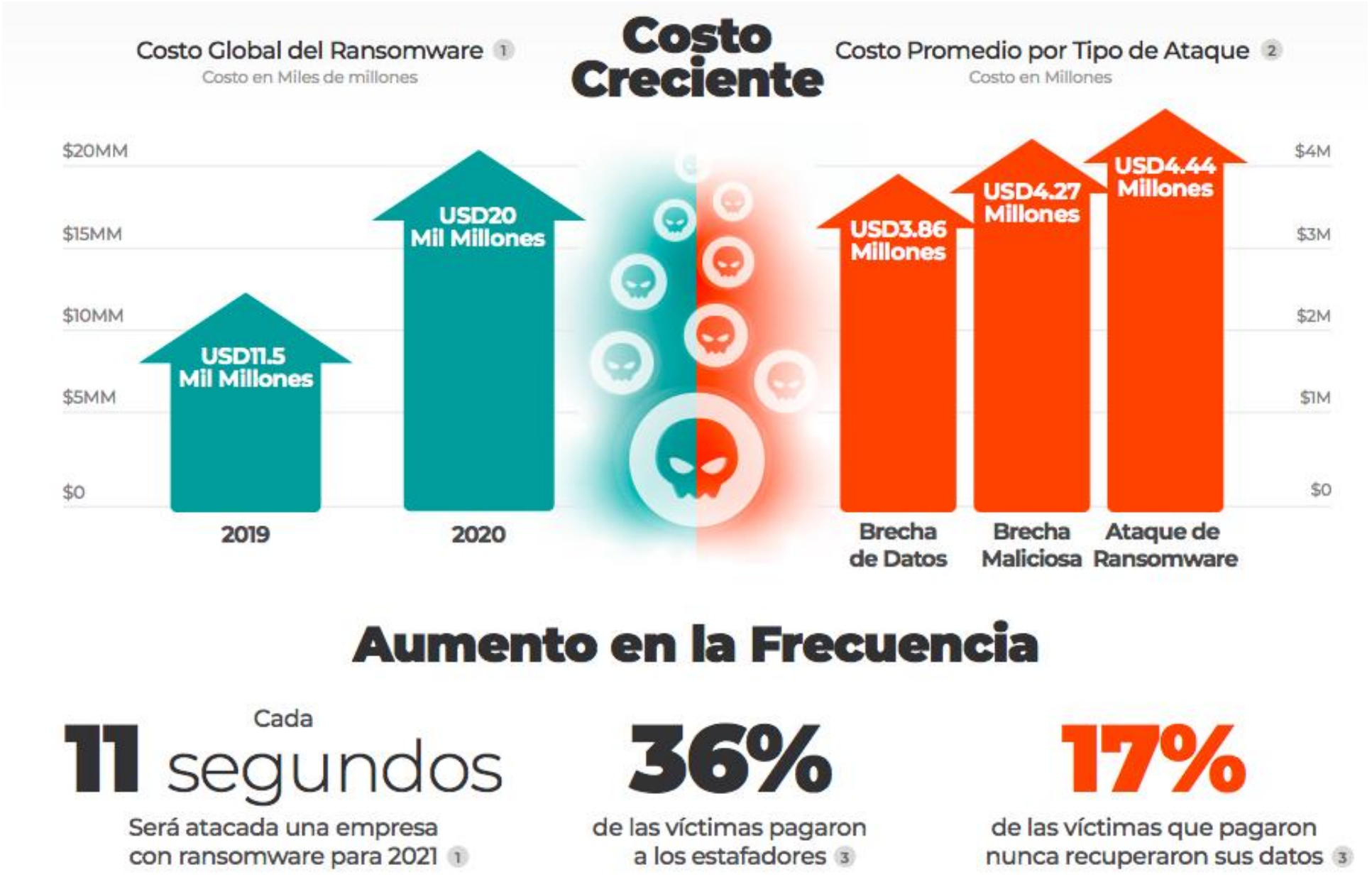
69%
Incremento en ciber ataques en el 2020

34%
De los ataques en el 2020 son internos

verizon

69%
De las empresas no están seguros de poder recuperarse

DELL EMC



Forbes

Aumento en la Frecuencia

Cada **11** segundos

Será atacada una empresa con ransomware para 2021 1

36%

de las víctimas pagaron a los estafadores 3

17%

de las víctimas que pagaron nunca recuperaron sus datos 3

DELL Technologies

Fuente: Ciberseguridad Riesgos, avances y el camino a seguir en América Latina y El caribe.

[CiberSeguridad (observatoriociberseguridad.org)]

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la Infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

www.observatoriociberseguridad.com

CIBERSEGURIDAD

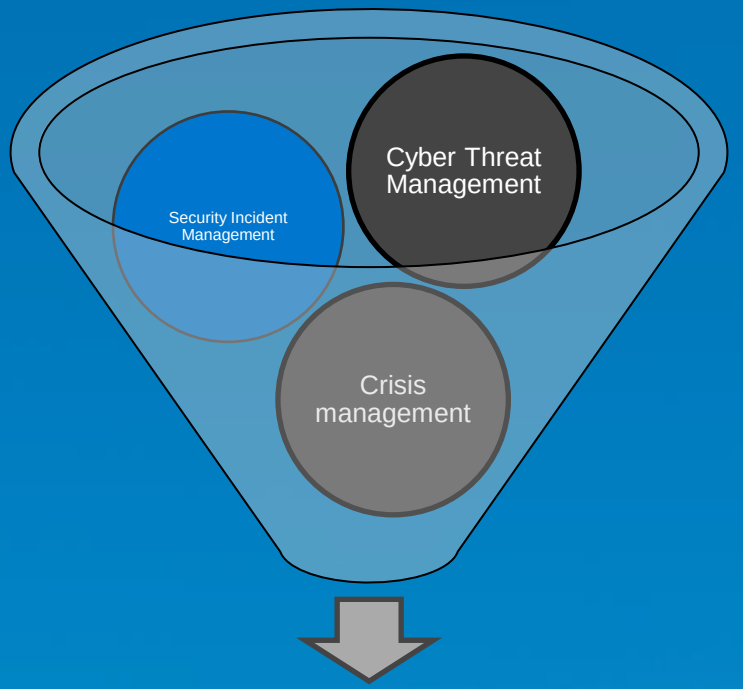
RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

DELL Technologies

Seguridad, una disciplina básica y relevante

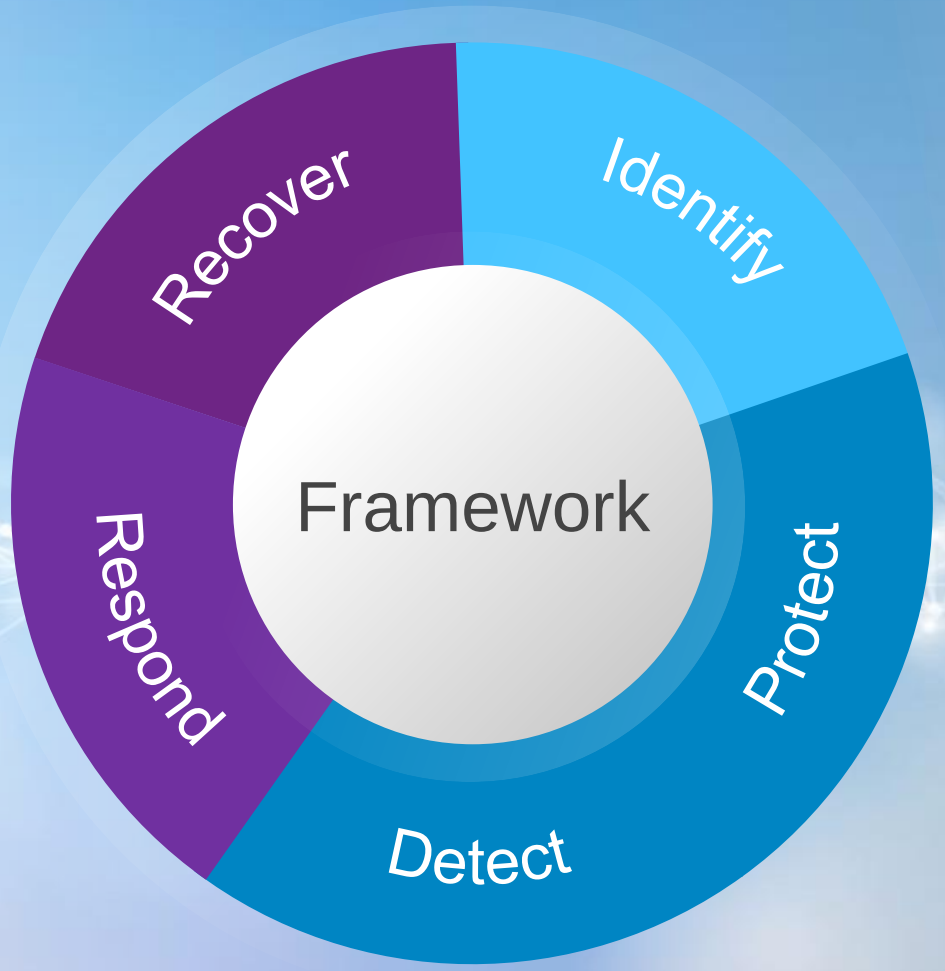
¿Qué es la resiliencia cibernética?

La forma en que una empresa u organización podrá mantener sus operaciones frente a algún tipo de ataque informático o ataque a la ciberseguridad, protegiendo no solo sus operaciones sino también su imagen y reputación corporativa.



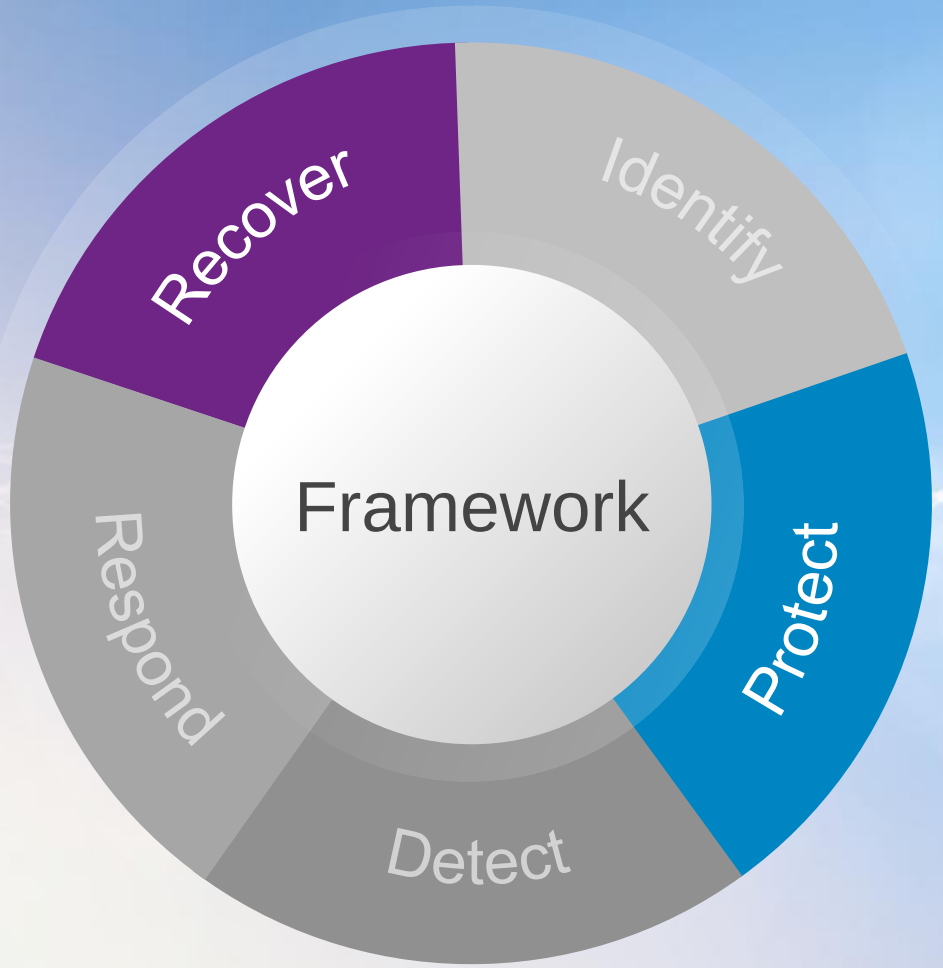
Estrategia de **Ciber Resilencia**

Una estrategia holística de alto nivel que incluye estándares de seguridad cibernética, pautas, personas, procesos comerciales y soluciones tecnológicas



Ejemplo: NIST Cybersecurity Framework

Source: https://en.wikipedia.org/wiki/Cyber_resilience



La Ciber Recuperación es la solución.

Una solución de protección de datos que aísla los datos críticos para la empresa de las superficies de ataque.

Los datos críticos se almacenan de forma inmutable en una bóveda digital que permite la recuperación con disponibilidad, integridad y confidencialidad de los datos

Source: https://en.wikipedia.org/wiki/Cyber_resilience

Gartner

Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware

Published 6 January 2021 - ID G00733304 - 20 min read

By Nik Simpson, Ron Blair

Recommendations

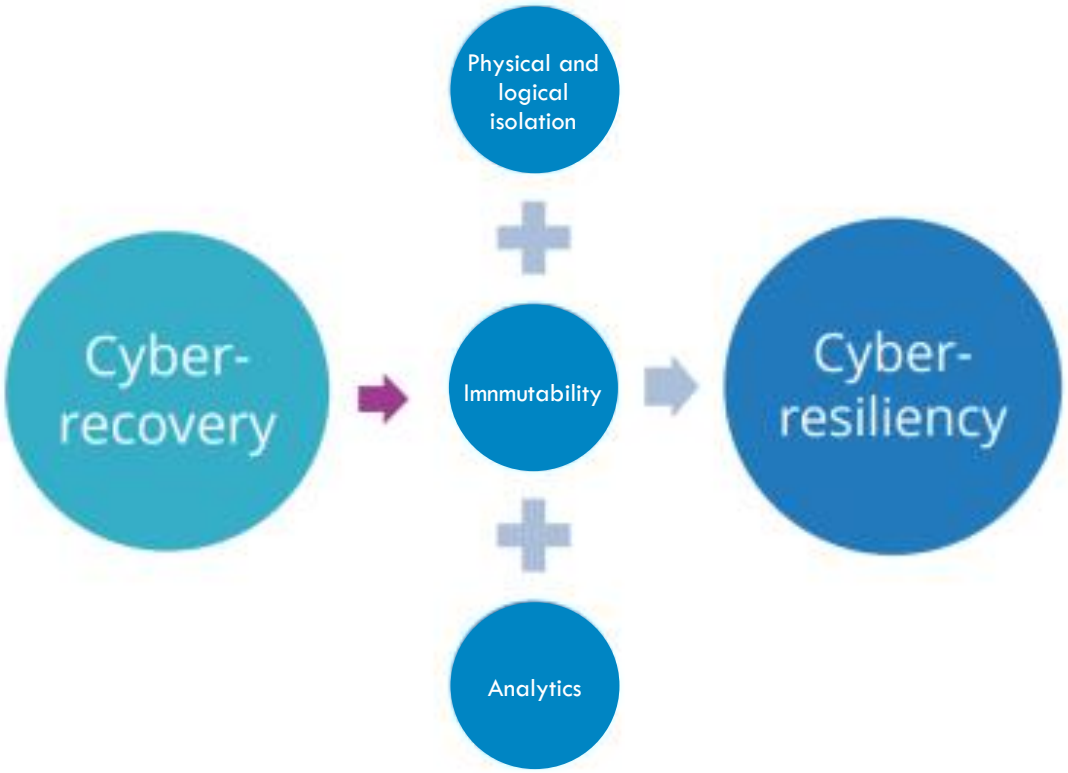
Infrastructure and operations leaders responsible for data center infrastructure must:

- Eliminate network sharing protocols — Avoid the use of simple network sharing protocols, such as CIFS or NFS when implementing storage for backup data.
- Protect the backup system — Protection of both the backup administration console and copies of backup data ensures usable backups are always available.
- Use multifactor authentication for administrative accounts — Implement two-factor authentication for all backup administrator accounts, and ensure that accounts are configured with the minimum privilege required to function.
- Create an isolated recovery environment — Make ransomware recovery via an IRE part of your disaster recovery plan, and include it in future disaster recovery tests.

DELL Technologies

Modern Cyberthreats Demand Comprehensive, Integrated Data Protection and Recovery Solutions

Foundational Requirements of Cyber-Resiliency



Cyber-resiliency. Cyber-resiliency is aimed at addressing both the traditional disaster and cyberattack recovery use cases. Cyber-resiliency encompasses the people, processes, and technology needed to recover compromised data and/or application services, regardless of the cause. Cyber-resiliency requires not only that data and application be recovered but also that system, application, and data integrity are ensured. It leverages known sources of validated uncorrupted data and/or malware/ransomware-free applications and systems prior to restoration of data and application services. Recovery responses can be for a single data store or application all the way up to entire systems similar to a disaster recovery response. As with disaster recovery, orchestration tools for recovery are commonly deployed. The act of leveraging a cyber-resiliency platform following a catastrophic event, whether that event is a cyberattack or disaster, is referred to as cyber-recovery.

Source: IDC, 2021

Misión de Sheltered Harbor’s

La iniciativa Sheltered Harbor fue lanzada por la industria en 2015 para garantizar que, en el peor de los casos:

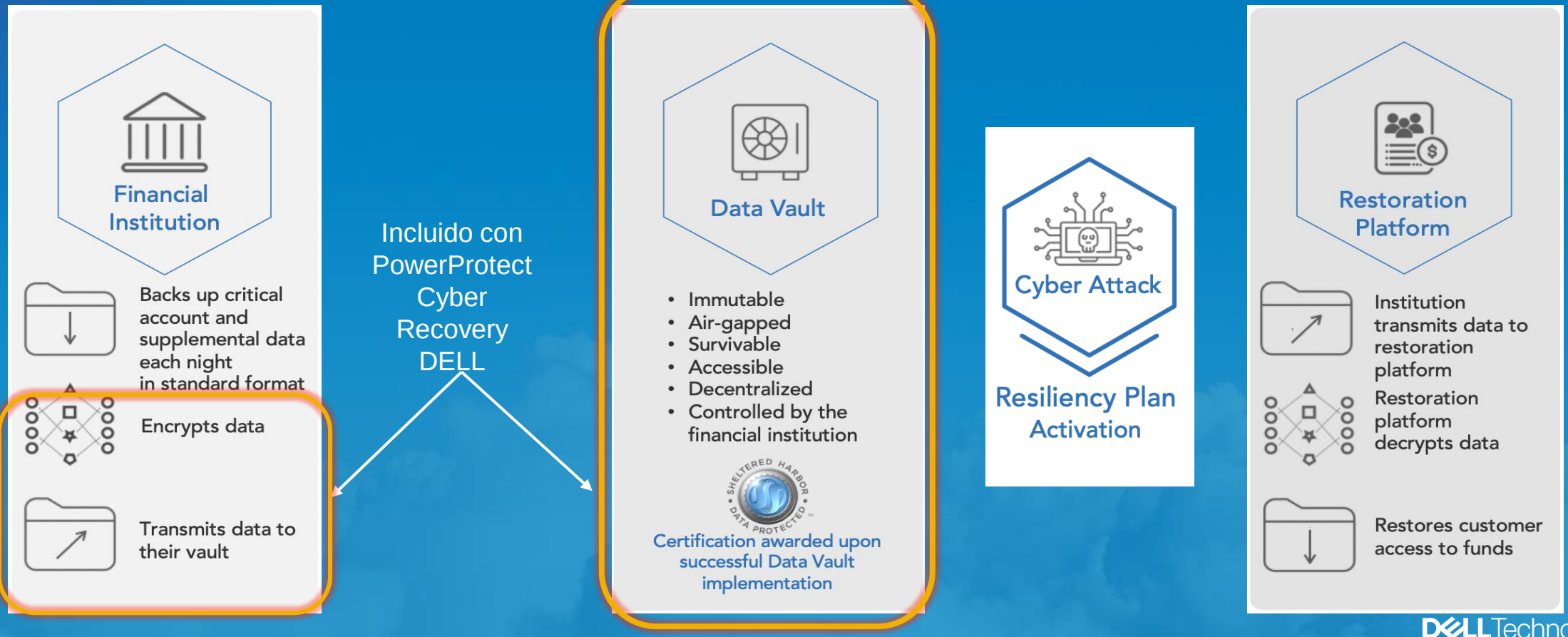
- Se mantenga la confianza pública en el sector financiero en USA
- Los conjuntos de datos críticos estarán protegidos en toda la industria
- Los servicios críticos podrán continuar incluso cuando los sistemas y los respaldos están inactivos
- Una institución financiera afectada tendrá un salvavidas para sobrevivir
- Todo lo anterior debe poder lograrse independientemente del origen del evento

Proceso de Protección de Datos de Sheltered Harbor

El participante realiza la extracción de los datos críticos de las cuentas de los clientes en el formato estándar de Sheltered Harbor

La bóveda de datos está encriptada, es inalterable y está completamente separada de las demás infraestructuras de la institución, incluidas las copias de seguridad

La recuperación y restauración seguras son independientes de los sistemas externos para reanudar rápidamente las operaciones comerciales



DELL Technologies

Atributos de una solución de Cyber Recovery

Ataques modernos requieren soluciones modernas y ágiles

Plan de activación de Ciber Resilencia

DELL Technologies


¿Su organización está preparada para resistir un ataque cibernético sofisticado?
Permítanos apoyarle somos DELL Technologies