Resiliencia del Dato

Contexto Actual y NIS2

José Luis García

Responsable Sector Público

SOCINFO sociedad de la información digital

Datos: la tormenta perfecta de complejidad y amenazas:

Explosion de datos y normativa

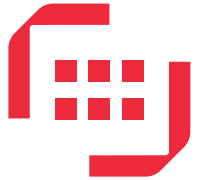
150+ ZB

Creados en 2024
se duplica cada año…IA

Complejidad de la Infraestructura

92%

Compañias tienen estrategia multi-cloud



Portabilidad Vendor Lock-In

Cada 3 Años

Actualización y renovacion de la infra HW&SW

Volumen y complejidad del Ransomware

1 de cada 4

28% pagan el rescate y no recuperan sus datos.

Complejidad

Amenazas

El 75% sufrió ataques de ransomware

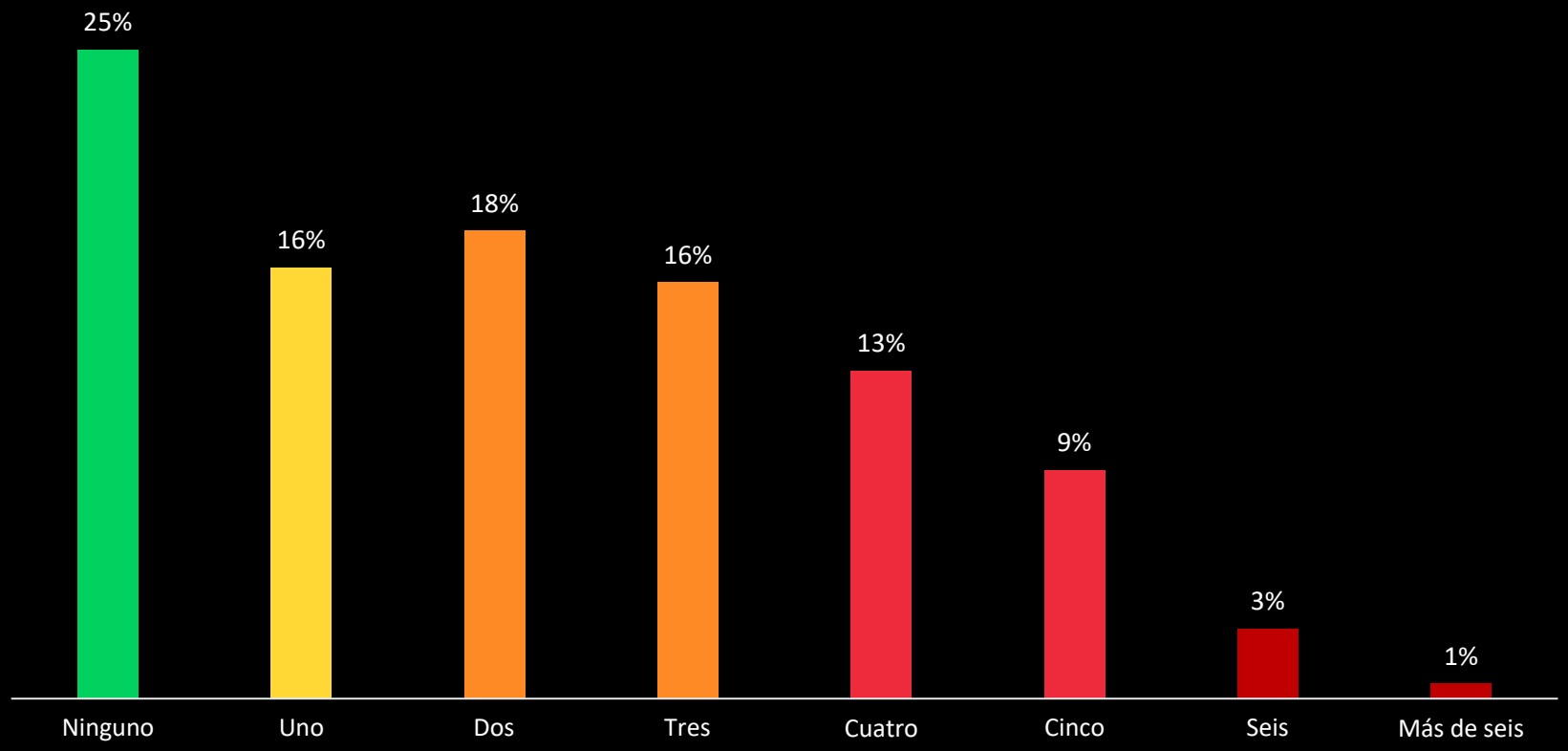
Más organizaciones sufrieron ataques trimestralmente (26%) que las que creen que no fueron atacadas en absoluto (25%)

92% encriptación de datos

76% exfiltración de datos

22 Días 100% recuperación

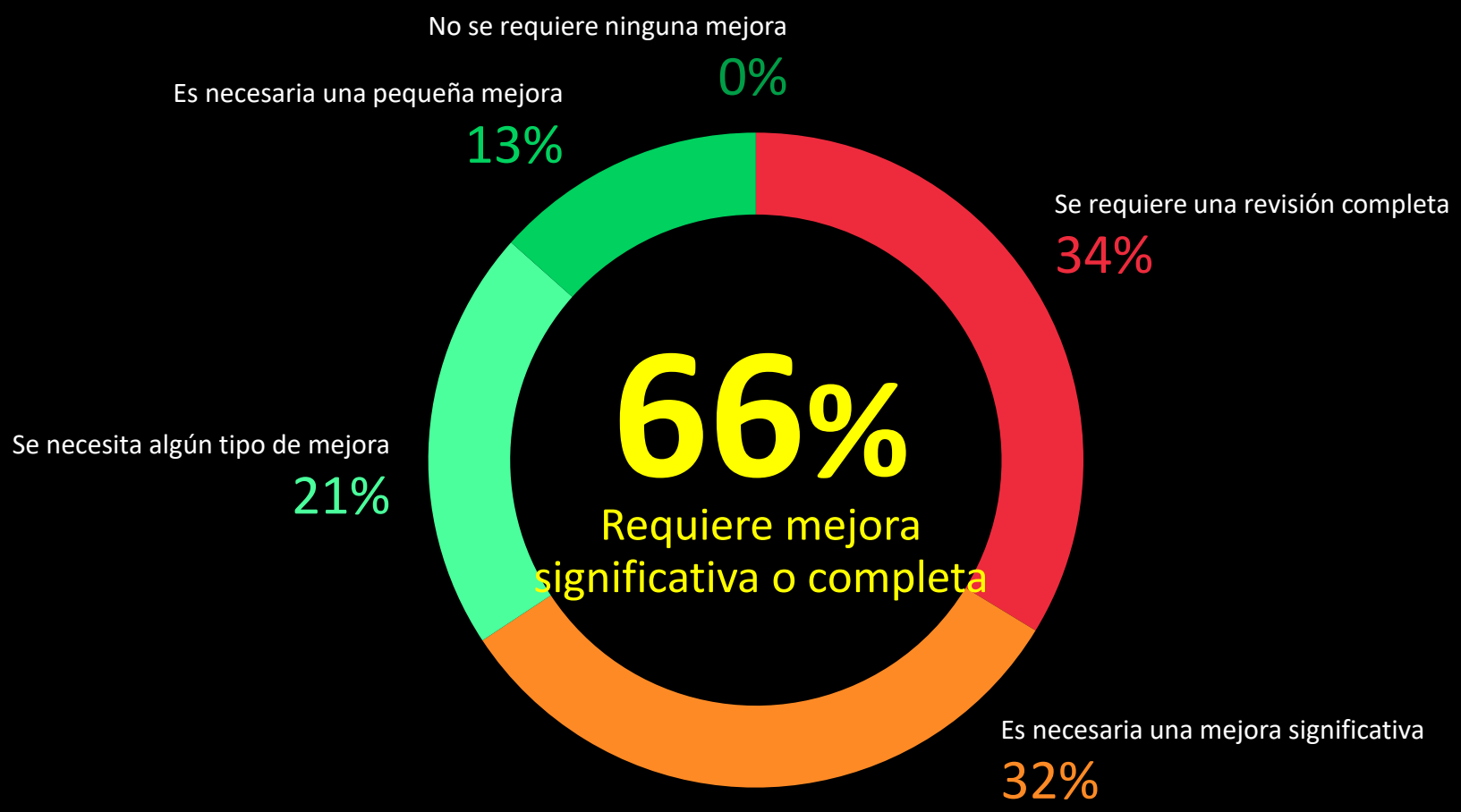
¿Cuántos ataques de ransomware ha sufrido su organización en los últimos 12 meses? (n=710)



Fuente: **Informe Tendencias Ransomware 2024**
https://vee.am/DPR24

Preparación de la organización (próximos pasos)

¿Cuánta mejora cree que es necesaria para que los equipos de ciberseguridad, de continuidad de negocio y de salvaguarda de la información de su organización estén debidamente alineados?



Fuente: **Informe Tendencias Ransomware 2024**
https://vee.am/DPR24

Las diez principales conclusiones

Informe de tendencias ransomware 2024

https://vee.am/R24

1. La ciberresiliencia **comienza en una sala de reuniones**, no en el centro de datos
2. Un incidente afectará a la organización pero **impactará mucho a las personas** que se ocuparán de solventarlo
3. El **rescate es un 38% del impacto financiero total** y está fuera del ciberseguro
4. Los **costes de los ciberseguros** siguen subiendo y las coberturas siguen bajando
5. Hay más organizaciones que “**pagaron pero NO pudieron recuperar**" que aquellas que “recuperaron SIN pagar"

veeam

Las diez principales conclusiones

Informe de tendencias ransomware 2024

https://vee.am/R24

6 Es probable que un **40% de los datos se vean afectados** por el ataque

7 Piense que **perderá el 18%** de sus datos

8 **NO siempre se puede usar su datacenter** y se debe recuperar en infra alternativa

9 **Los repositorios de backup fueron el objetivo en el 96%** de los ataques y fueron afectados en el 76% de ellos

10 Es crítico un backup sólido y **verificado con pruebas de recuperación rutinarias**

¿Estamos preparados para proteger el servicio o negocio ?

1 dólar en

44 dólares en

ee que el cibercrimen
sferencia de riqueza
la historia

36% incremento presupuestos ciber recovery/resiliency

Source: IDC Future Enterprise Resiliency & Spending Survey September 2024

La directiva NIS2

Requisitos/Medidas de NIS2…

- ✓ Las organizaciones deben llevar a cabo **análisis de riesgos y establecer políticas de seguridad para los sistemas de información**.
- ✓ Las organizaciones deben implementar medidas robustas de **protección de datos y recuperación ante desastres**
- ✓ Las organizaciones deben adoptar prácticas sólidas de **gestión de riesgos de la cadena de suministro (proveedores)**

…orientadas a asegurar que se puedan **restaurar datos y reanudar operaciones rápidamente** tras un incidente de ciberseguridad.

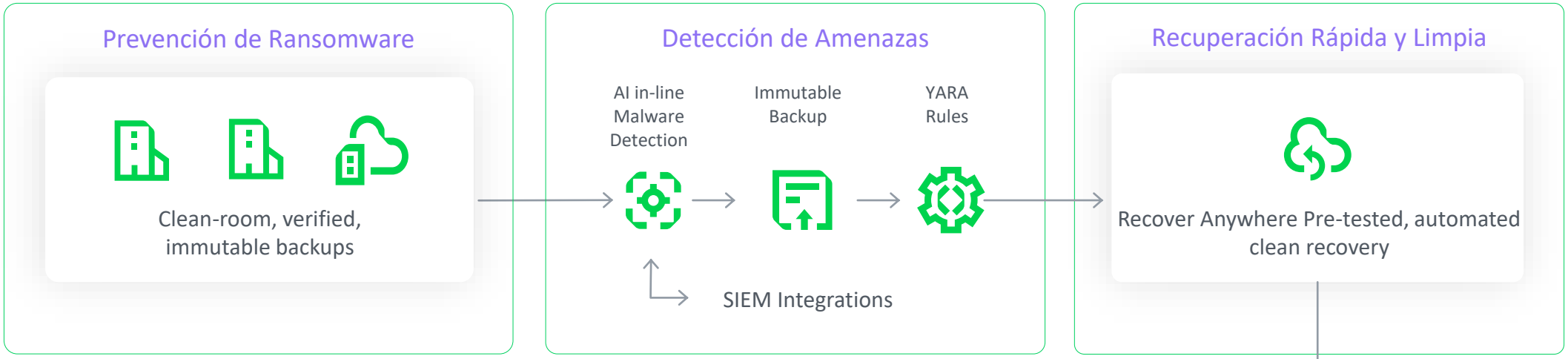
Veeam

diseñado para incrementar la resiliencia de los datos y el servicio (público)

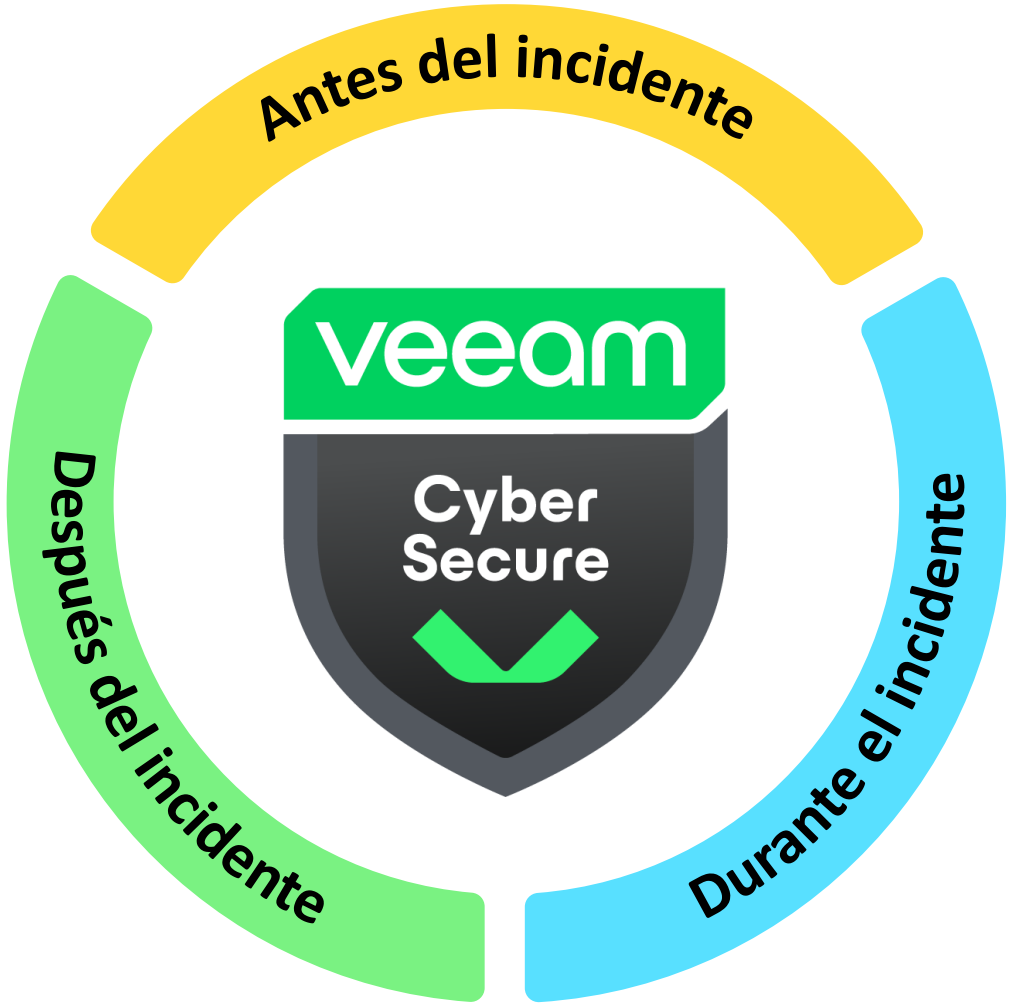
Veeam provee la más completa protección y recuperación end-to-end contra el ransomware

Veeam Cyber Secure Program

24/7/365 SWAT Team | Health Checks | Ransomware Warranty | Incident Response Retainer



La mayor base de datos commercial sobre Cyber Incident Data



Soporte completo para cada etapa del incidente

Antes del incidente

- Servicios de diseño e implementación
- Asistencia avanzada durante onboarding
- Evaluaciones trimestrales de seguridad

Durante el incidente

- Enrutamiento prioritario y SLA de 15 min 24x7
- Gestor de cuenta de soporte dedicado
- Veeam SWAT team de respuesta ransomware
- Descifrado, recuperación, negociación y acuerdo (legal)

Después del incidente

- Para ataques verificados, hasta cinco millones de dólares (USD) de garantía de reembolso para gastos de recuperación

Veeam Cyber Resilient Ecosystem

Security information and event management (SIEM)

SOPHOS · paloalto NETWORKS · splunk> a CISCO company · CROWDSTRIKE

veeam Event Forwarding

Security Orchestration, Automation and Response (SOAR)

servicenow · paloalto NETWORKS · Progress Flowmon · PREDATAR · Cisco XDR · valicyber

veeam Incident API

SureBackup Light & Secure Restore

Bitdefender · eset · Microsoft Defender · SOPHOS · Symantec by Broadcom · Trellix

Incident Response

veeam Cyber Secure with coveware by veeam

YARA – rule-based detection

veeam

Recon

coveware by veeam

Ransomware detection

Bitdefender · eset · Microsoft Defender · SOPHOS · Symantec by Broadcom · Trellix · veeam

Immutability for Backups & Primary Storage Snapshots

Immutable Snapshots

Hewlett Packard Enterprise · IBM · INFINIDAT · lenovo · NetApp · PURESTORAGE

Immutable Backups

II:II SYSTEMS · aws · Azure · BACKBLAZE · ceph · cisco · CLOUDIAN · DATACORE · DELL · EXAGRID · FUJITSU · Hewlett Packard Enterprise · HITACHI · IBM · IBM Cloud · IDrive · Impossible Cloud · INFINIDAT · Infortrend · iTernity · lenovo · MINIO · NetApp · NEXSAN · NUTANIX · OBJECT FIRST · OSNEXUS · OVHcloud · PURESTORAGE · QNAP · Quantum · Quest · Red Hat · RSTOR · SCALITY · SEAGATE · SOFTIRON · SPECTRA · STONEFLY · SUPERMICRO · SUSE · SWARM · SwiftStack · Synology · Ugloo · VAST · wasabi · zadara · veeam

Immutable Backup Copies

II:II SYSTEMS · aws · Azure · BACKBLAZE · ceph · cisco · CLOUDIAN · DATACORE · DELL · EXAGRID · FALCONSTOR · FAST LTA · FUJITSU · Hewlett Packard Enterprise · HITACHI · IBM · IBM Cloud · IDrive · Impossible Cloud · INFINIDAT · Infortrend · iTernity · lenovo · MINIO · NetApp · NEXSAN · NUTANIX · OBJECT FIRST · OSNEXUS · OVERLAND TANDBERG · OVHcloud · POINT · PURESTORAGE · QNAP · Quantum · Quest · Red Hat · RSTOR · SCALITY · SEAGATE · SOFTIRON · SPECTRA · StarWind · STONEFLY · SUPERMICRO · SUSE · SWARM · SwiftStack · Synology · Ugloo · VAST · wasabi · zadara · veeam

Storage & Backup Compliance Monitoring

CONTINUITY · veeam

Readiness

DARKTRACE · kyndryl · PREDATAR · elastio · PAESSLER THE NETWORK MONITORING COMPANY

Encryption/KMS

ENTRUST · Fortanix · IBM Security · THALES · aws · Azure · Google Cloud

veeam

Veeam & NIS2 en resúmen

Veeam Backup & Replication
Protege los datos contra pérdidas y amenazas al proporcionar backup y replicación fiables para todas las cargas de trabajo.

Veeam ONE
Proporciona monitorización avanzada, informes y planificación de capacidad para su entorno.

Veeam Threat Center
Destaca las amenazas, identifica los riesgos y mide la puntuación de seguridad de tu entorno

Veeam Security & Compliance Analyzer
Supervisa el estado de la infraestructura para una recuperación exitosa con análisis automatizados, en base a las mejores prácticas de protección de datos.

Veeam Recovery Orchestrator
Garantiza una recuperación orquestada de servicios críticos con recuperación, planificación y pruebas ante desastres automatizadas.

Veeam: Certificaciones y Guías de Seguridad

[BP/34 Recomendaciones de Seguridad sobre Veeam Data Platform]

Recomendaciones de Seguridad sobre Veeam Data Platform

National Institute of Standards and Technology
U.S. Department of Commerce

Section508.gov

GSA Government-wide IT Accessibility Program

- ISO 27001 certified, certificate #2021-122101
- SOC2 L1, L2 cert in progress
- TAA compliant
- NIST CSRC FIPS 140-2 certified encryption module
- GSA VPAT Section 508 compliance

- Hardened Linux Repository: SEC 17a-4(f), FINRA 4511(c) and CFTC 1.31(c)-(d) WORM compliant
- DoDIN APL
- Common Criteria in process via NIAP
- CACI Code Guardian

https://aplits.disa.mil/processSchedule
https://www.niap-ccevs.org/Product/PINE.cfm
https://www.veeam.com/blog/exploring-it-security-certifications.html

Market Leader

#1

IDC in the Data Replication & Protection

#1

Gartner Magic Quadrant Leader

81%

Fortune 500

+75

Net Promoter Score

https://go.veeam.com/business-value-platform