semperis

SUPLEMENTO PARA ESPAÑA

2024

# Informe sobre el riesgo de ransomware durante las vacaciones

- Orientación especializada para fortalecer las defensas frente al ransomware, especialmente durante los periodos de alto riesgo como las vacaciones, los fines de semana y las transiciones empresariales
- Estudio de los patrones de ataque de los secuestros de datos que revela que muchas organizaciones no tienen las defensas adecuadas frente a ataques que tienen lugar cuando hay distracciones
- Nueva evidencia de que las organizaciones habitualmente sobrestiman su capacidad para defenderse frente a ataques asados en la identidad

"Durante las vacaciones y los fines de semana, las empresas no deben relajar sus defensas, sino que deben aumentar su vigilancia frente a los ciberataques. Los cibercriminales a menudo explotan estos periodos con personal reducido para lanzar ataques de ransomware. La manera más efectiva de protegerse frente a estas amenazas es mediante una mayor concienciación y un plan exhaustivo de respaldo y recuperación de los datos que se pueda implementar rápidamente cuando sea necesario."

**Ray Mills**
Director, Semperis

# El riesgo de **ransomware**

**Los ataques de ransomware no respetan el horario laboral y los ataques suelen producirse con tal velocidad que la intervención humana es insuficiente por sí sola. Por lo tanto, se necesitan compendios de identidad automatizados para mitigar el riesgo.**

Los responsables de los ataques actúan durante los periodos de ausencia o distracción, por ejemplo, durante las vacaciones, los fines de semana y acontecimientos empresariales, que incluyen las fusiones y las adquisiciones.

Las organizaciones de todo el mundo están librando una batalla contra los secuestros de datos y otros ciberataques. A medida que aumentan los riesgos, también crece la evidencia de que Microsoft Active Directory es uno de los objetivos principales de los responsables de estos ataques y de que la detección y respuesta a las amenazas de identidad (ITDR, por sus siglas en inglés) es un aspecto clave de la resilencia cibernética y operativa.

Para examinar las tendencias en la frecuencia, gravedad e impacto del ransomware, Semperis se asoció con la empresa de investigación internacional Censuswide para realizar un estudio exhaustivo que abarca múltiples industrias en los Estados Unidos, el Reino Unido, Francia y Alemania. El primer informe de nuestros resultados—*2024 Ransomware Risk Report (Informe sobre el riesgo de secuestro de datos en 2024)*—reveló que estos ataques son incesantes y costosos. Un segundo informe—*2024 Ransomware Holiday Risk Report (Informe sobre el riesgo de secuestro de datos durante las vacaciones de 2024)*—examinó la cadencia de los ataques que tienen lugar durante periodos de distracción empresarial (incluidas las vacaciones, los fines de semana y eventos relevantes tales como fusiones, OPI y despidos) y los posibles lapsos en las defensas de la seguridad cibernética de las organizaciones.

**Este suplemento expande nuestro estudio. Pedimos a 100 organizaciones en España que contestaran un subconjunto de las preguntas de nuestro estudio para determinar su experiencia con los temas cubiertos en los informes previos.**

## EXPERTOS CONTRIBUYENTES


**Mickey Bresman**
CEO de Semperis

**Ray Mills**
Director de Semperis

**Guido Grillenmeier**
Tecnólogo principal de Semperis (EMEA)

**Simon Hodgkinson**
Consejero estratégico de Semperis, exdirector de seguridad informática de bp

**Chris Inglis**
Consejero estratégico de Semperis, exdirector cibernético nacional de los EE.UU.

# Los atacantes no toman vacaciones

"Cuando los atacantes entran en los sistemas de la empresa, especialmente si lo hacen en un fin de semana durante las vacaciones cuando hay menos personal, puede que su presencia no se detecte inmediatamente. Las empresas prestan menos atención y son más vulnerables durante estos periodos y los atacantes lo saben."

**Guido Grillenmeier**
Tecnólogo principal (EMEA), Semperis

**75%**

**de las organizaciones que sufrieron ransomware fueron atacadas durante un fin de semana o feriado**

**EDUCACIÓN**
**100%**

**MANUFACTURA**
**33%**

**FINANZAS**
**92%**

**INFORMÁTICA/ TELECOMUNICACIONES**
**73%**

**ATENCIÓN SANITARIA**
**100%**

**VIAJES/TRANSPORTE**
**50%**

# Los atacantes actúan cuando el personal del Centro de Operaciones de seguridad (SOC) está reducido

## ¿Mantiene su empresa un SOC las 24 horas del día los 365 días del año?

**95%**
**SÍ**

> "La seguridad cibernética no puede aumentar y disminuir. Debe mantenerse constante y estar presente siempre."
>
> **Chris Inglis**
> Consejero estratégico de Semperis, exdirector cibernético nacional de EE.UU.

| | TODAS | EDUCACIÓN | FINANZAS | ATENCIÓN SANITARIA | MANUFACTURA | INFORMÁTICA/ TELECOMUNI-CACIONES | VIAJES/ TRANSPORTE |
|---|---|---|---|---|---|---|---|
| **Sí (total)*** | **94%** | **100%** | **92%** | **100%** | **100%** | **96%** | **75%** |
| Sí *(subcontratado/híbrido)* | **27%** | 50% | 25% | 50% | 100% | 23% | 25% |
| Sí *(interno)* | **68%** | 50% | 67% | 50% | | 73% | 50% |

## ¿Reduce el personal del SOC durante los fines de semana y los feriados? Si lo hace, ¿en qué proporción?

**84%** de los encuestados **reducen** su personal en **hasta un 50%**

Las organizaciones en la industria de la informática/telecomunicaciones tenían una probabilidad mayor de **mantener el personal** de

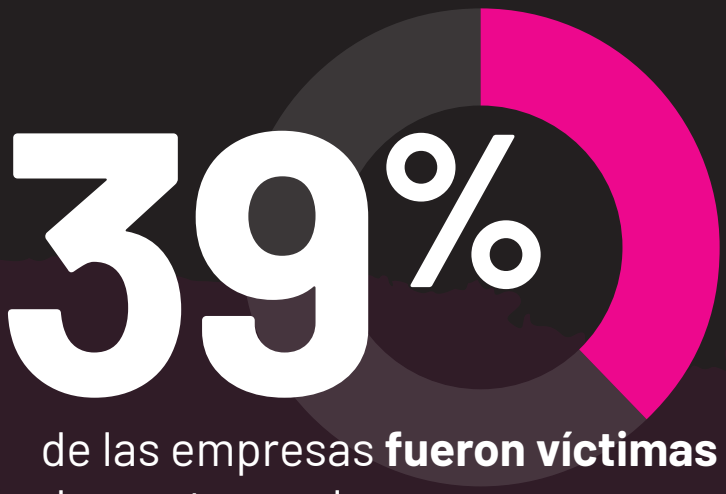
**50%** **O MÁS** durante los fines de semana y los feriados.

**65%** de las organizaciones que **reducen** el personal de SOC durante los fines de semana y los feriados lo hacen para **proteger el equilibrio entre la vida laboral y personal**

# Los ataques ocurren durante los periodos de distracción empresarial

"No me sorprende en absoluto el porcentaje de organizaciones que sufren un ataque después de un evento empresarial... Durante eventos relevantes, la prioridad de la empresa es completar el evento, no la seguridad."

**Simon Hodgkinson**
Consejero estratégico, Semperis
exdirector de seguridad informática de bp



**39%**

de las empresas **fueron víctimas** de un ataque de ransomware **después de un evento empresarial relevante**

**EDUCACIÓN**
**50%**

**MANUFACTURA**
**33%**

**INFORMÁTICA/ TELECOMUNICACIONES**
**37%**

# La protección de la identidad es crucial para la resilencia del negocio

"Sustituya con la siguiente cita: "Mientras muchas organizaciones se centran en la protección de los puntos finales, los atacantes a menudo eluden por completo estas defensas. Una vez dentro, atacan el sistema de identidad, el backbone de su red. Una vez que la infiltran, tienen control de la totalidad de su infraestructura. Sin un sistema de identidad resiliente, todas las demás defensas se vuelven inefectivas."

**Ray Mills**
Director, Semperis

**82%**

**TIENEN UN PRESUPUESTO ESPECÍFICAMENTE PARA LA DEFENSA DE LOS SISTEMAS DE IDENTIDAD FUNDAMENTALES COMO ACTIVE DIRECTORY**

**¿Cuánto tiempo tardaron las empresas en recuperar una funcionalidad informática mínima?**

- **23%** MENOS DE 5 HORAS
- **26%** 1-7 HORAS
- **49%** 5 HORAS - 1 DÍA
- **2%** MÁS DE 7 DÍAS

**94%**

de los encuestados dicen haber implementado un **plan de recuperación de la identidad**

- EDUCACIÓN **100%**
- FINANZAS **92%**
- ATENCIÓN SANITARIA **75%**
- MANUFACTURA **100%**
- INFORMÁTICA/ TELECOMUNICACIONES **96%**
- VIAJES/TRANSPORTE **75%**

# Cómo alinear las prioridades de la empresa

**Los ataques de ransomware informáticos pueden ocurrir, y de hecho ocurren, cuando menos se espera. Ninguna empresa, independientemente de la región, el sector, o el estado de su SOC, debe subestimar la necesidad de mantener una vigilancia constante. Además, para que los esfuerzos de defensa contra el ransomware tengan éxito deben incluir un plan claro de defensa y recuperación del Active Directory. Teniendo esto en cuenta, ¿qué pasos pueden tomar los líderes de la empresa, tecnología y seguridad para reducir la probabilidad de que un ataque de ransomware tenga éxito y aumentar su capacidad de decir "no" a los responsables de estos ataques? Nuestros expertos sugieren tres acciones iniciales.**

## PASO 1

Los directivos de más alto nivel deben reconocer que **la defensa frente al ransomware** y la **seguridad de la identidad** son **prioridades de la empresa.**

## PASO 2

**Contar con soluciones ITDR robustas** y **socios expertos** puede ayudar a los directores de seguridad a **compensar los retos en materia de personal.**

## PASO 3

**La seguridad del Active Directory** debe ser **un aspecto principal** de cualquier fusión o adquisición.

"El conocimiento del papel crítico que la identidad juega en la historia de la seguridad ha aumentado significativamente en los últimos años. Aunque la ITDR está finalmente recibiendo la atención que se merece, todavía queda mucho por hacer en cuanto a la protección y seguridad de los sistemas de identidad."

**Mickey Bresman**
CEO, Semperis

## METODOLOGÍA

Para realizar este estudio, nos asociamos con expertos de Censuswide, una empresa de consultoría internacional de investigación de mercados con sede en Londres. Censuswide encuestó a 100 profesionales de informática y seguridad en España, en las industrias de educación, finanzas, atención sanitaria, manufactura y servicios, informática y telecomunicaciones, y viaje y transporte.

## CÓMO CITAR LA INFORMACIÓN CONTENIDA EN ESTE INFORME

Los datos de este informe se proporcionan como fuente de información para la comunidad de la seguridad informática y las organizaciones a las que sirve. Semperis le anima a que comparta nuestros resultados. Para citar las estadísticas u otros datos, mencione *el Informe sobre el secuestro de datos durante las vacaciones: suplemento para España* publicado por Semperis e incluya el enlace al informe, que se puede bajar en https://www.semperis.com/resources/espana-ransomware-risk. Para entrevistar a los expertos de Semperis, póngase en contacto con Bill Keeler en billk@semperis.com. Por último, nos gustaría que compartiese con nosotros sus preguntas y comentarios sobre el ransomware y la resilencia. Visite Semperis en LinkedIn.

## ACERCA DE SEMPERIS

Semperis garantiza la integridad y disponibilidad de los servicios de directorio empresarial críticos en cada paso de la cadena de eliminación cibernética, lo que permite a los equipos de seguridad encargados de proteger entornos híbridos y multinube reducir el tiempo de recuperación en un 90%. La tecnología patentada de Semperis, desarrollada específicamente para proteger entornos de identidad híbridos, incluidos Active Directory, Entra ID y Okta, protege más de 100 millones de identidades contra los ataques cibernéticos, las violaciones de datos y los errores operativos. Las organizaciones líderes del mundo confían en Semperis para detectar las vulnerabilidades de los directorios, interceptar ataques cibernéticos en curso y recuperarse con rapidez después de un secuestro u otro incidente relacionado con la integridad de los datos. La sede de Semperis está ubicada en Hoboken, New Jersey y opera internacionalmente, con un equipo de investigación y desarrollo distribuido a lo largo de los Estados Unidos, Canadá e Israel.

Semperis es la anfitriona de la galardonada conferencia y serie de pódcast Protección híbrida de la identidad (Hybrid Identity Protection) y ha desarrollado las herramientas de defensa cibernética del Active Directory híbrido de la comunidad, Purple Knight y Forest Druid. La empresa ha recibido el mayor nivel de elogios en al industria, fue incorporada recientemente a la lista de los mejores lugares de trabajo en 2024 de Inc. Magazine y fue nombrada la empresa de ciberseguridad con mayor crecimiento en América por el Financial Times. Semperis es socia de Microsoft Enterprise Cloud Alliance y Co-Sell y miembro de Microsoft Intelligent Security Association (MISA).

Más información: https://www.semperis.com

semperis

+1-703-918-4884 | info@semperis.com | www.semperis.com
5 Marine View Plaza, Suite 102, Hoboken, NJ 07030