Experis®
ManpowerGroup

Continuidad **operativa**, **productividad** de empresas y **solución** a brechas digitales mediante **centros de operación de redes (NOC)**

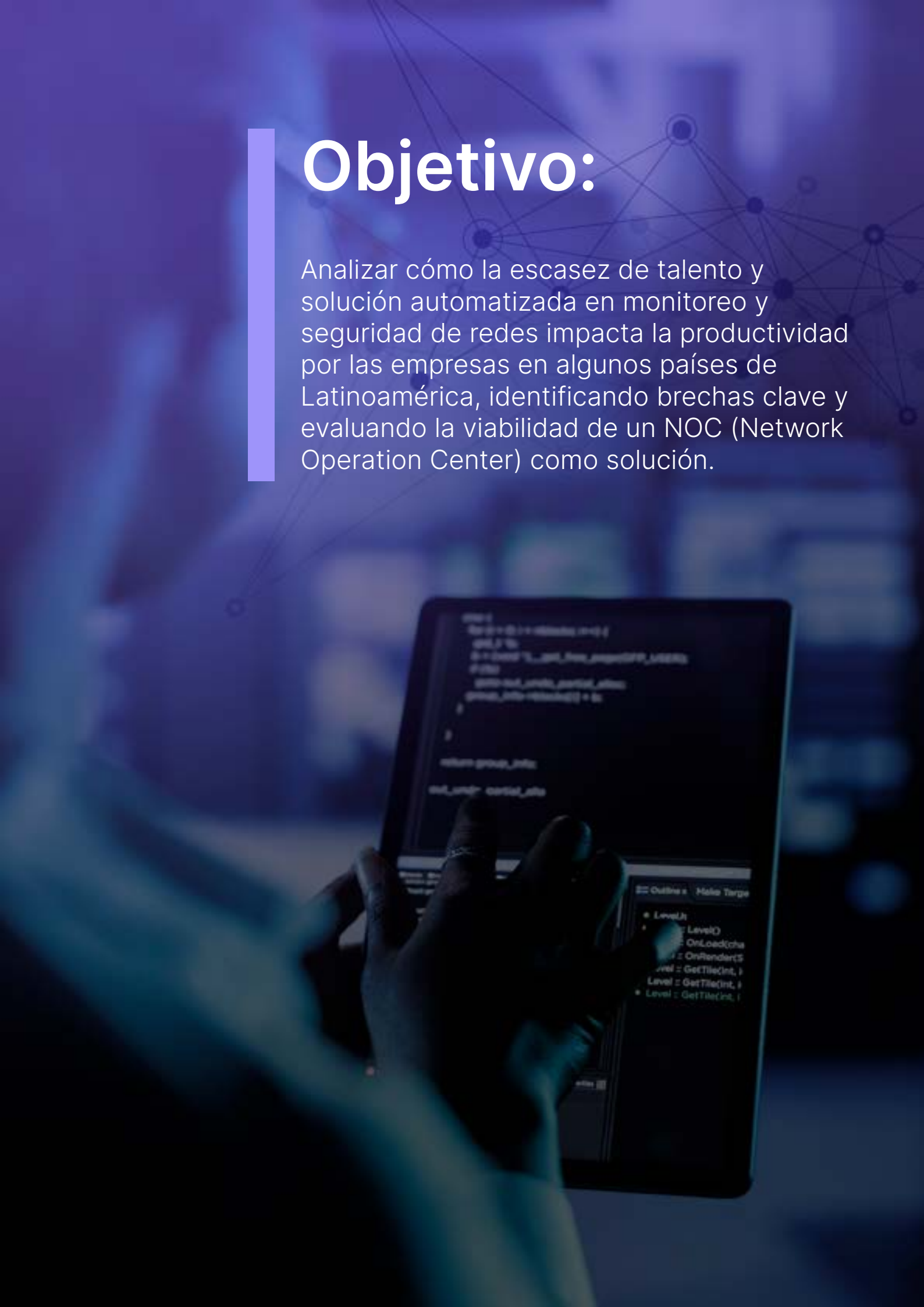
Experis LATAM

CONTENIDOS

Objetivo	**3**
¿Qué es un NOC?	**4**
Brechas en monitoreo y soporte de redes	**5**
Déficit de talento en monitoreo y seguridad de redes	**7**
Impacto de los fallos en la continuidad operacional	**10**
Ciberseguridad y amenazas emergentes	**16**
Insights y perfiles recomendados	**17**
Referencias	**19**

Objetivo:

Analizar cómo la escasez de talento y solución automatizada en monitoreo y seguridad de redes impacta la productividad por las empresas en algunos países de Latinoamérica, identificando brechas clave y evaluando la viabilidad de un NOC (Network Operation Center) como solución.



¿Qué es un NOC?

Un **NOC** (Network Operations Center), o **Centro de Operaciones de Red**, es una ubicación centralizada donde un equipo de profesionales de TI monitorea, gestiona y optimiza las redes de una organización las 24 horas del día, los 7 días de la semana. Su objetivo principal es garantizar que la infraestructura de red cumpla con los acuerdos de nivel de servicio (SLA) y satisfaga las necesidades comerciales de la empresa.

Funciones Principales del NOC

Monitoreo y Gestión de Redes:

El NOC supervisa continuamente el rendimiento y la seguridad de las redes, utilizando herramientas avanzadas para detectar problemas potenciales antes de que afecten las operaciones. El equipo del NOC trabaja para escalar y resolver incidentes técnicos, como fallas de hardware o software, y garantiza que la red esté disponible y funcione correctamente.

A través de la implementación de Bot RPA (automatización robótica de procesos) para realizar tareas repetitivas y configurado a los SLAs del mercado, permite minimizar fallas y garantizar los tiempos de respuesta.

Realizan tareas de optimización y mantenimiento preventivo para asegurar que la red opere de manera eficiente y sin interrupciones. Aunque el NOC se centra en la gestión de redes, colabora estrechamente con otros equipos, como el SOC (Centro de Operaciones de Seguridad), para abordar amenazas cibernéticas y garantizar la seguridad general del entorno TI.

Brechas en monitoreo y soporte de redes

Perspectiva regional de inversiones en ciberseguridad

Según medios especializados en Latinoamérica los países más afectados en 2024 corresponden a México, Brasil, Colombia y Perú.

Sólo **México** y **Brasil** concentran más del **45%** de los ataques.

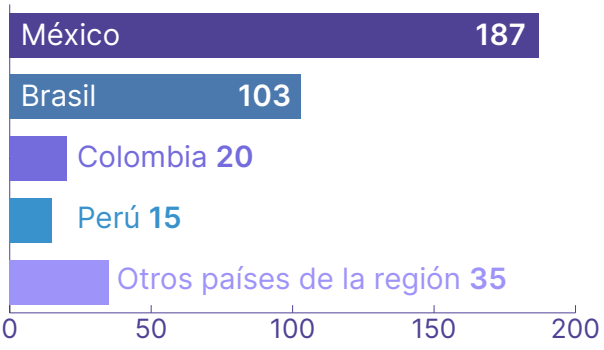
Según la multinacional tecnológica Tivit, las metas de los ciberataques son el beneficio económico **(33%)**, la denegación de servicio **(31%)** y el robo de datos **(22%)** y otros **(14%)**.

El Índice Global de Ciberseguridad mide el compromiso de los países con la ciberseguridad a nivel global (considerando lo público y privado)

Se evalúa en función de cinco pilares: legales, técnicas, organizativas, Desarrollo de capacidades y Cooperación.

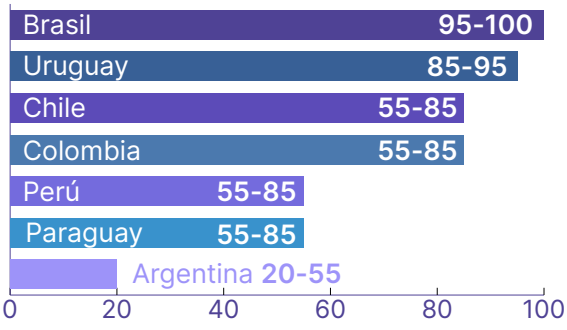
En la región, existe una correlación entre el nivel de desarrollo económico, cantidad de amenazas registradas y el índice, mostrando que los principales países afectados por el ciber crimen son los de economías más grandes y mayor exposición digital.

Cantidad de ciberataques registrados en 2024



Fuentes:
1.- Panorámica de la ciberseguridad en Latinoamérica – Ciberilatam
2.- Global Cybersecurity Index 2024

Índice de ciberseguridad 2024



Fuentes:
1.- Panorámica de la ciberseguridad en Latinoamérica – Ciberilatam
2.- Global Cybersecurity Index 2024

¿Cómo priorizan la inversión en monitoreo y soporte?

Ranking de tecnologías que las empresas planean adoptar:

1. Zero Trust
2. Procesos de gestión de riesgos de terceros
3. Marco de gobernanza de la información en toda la empresa
4. Capacidades de inteligencia de amenazas en tiempo real
5. Acceso definido por software
6. Gestión de identidades y accesos de consumidores
7. Gestión de identidades y accesos de consumidores
8. Planificación de la continuidad del negocio y recuperación
9. Servicios de seguridad gestionados
10. Seguridad de endpoints
11. Capacitación en concientización sobre seguridad y operaciones
12. Seguridad en la nube

Fuentes:
1.- Cybersecurity: market data & análisis, STATISTA (octubre, 2023)
2.- Reporte de Ciberseguridad, OCEAN, Entel (2023)

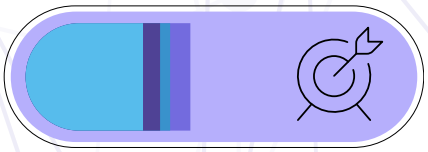
¿Cuáles son las principales barreras para una supervisión efectiva de redes y sistemas críticos?

Según el reporte OCEAN de Entel sobre ciberseguridad, para el cierre del año 2023 las empresas consideraban como barreras de entradas los siguientes ítems:

40%
Falta de personal y recursos calificados

33%
Cumplimiento legal y regulatorio

31%
Seguridad de datos, pérdida y riesgo de filtraciones



30% - Integración con ecosistema IT existente
26% - Miedo al bloqueo por parte del proveedor
24% - Riesgos generales de seguridad
21% - Pérdida de control

Déficit de talento en monitoreo y seguridad de redes

¿Cuántas empresas tienen dificultades para contratar personal calificado en monitoreo y ciberseguridad?

No hay un estimado de empresas con dificultades para contratación, pero si sentimiento de mercado de las grandes empresas.

30% de organizaciones sufrió al menos un incidente de redes o ciberataque desde 2023

23% de las empresas tiene contratado un seguro en caso de riesgos cibernéticos

63% de las organizaciones considera que el presupuesto asignado para redes y ciberseguridad es deficiente

85% de las grandes empresas cuenta con servicios de soluciones backup

83% de las grandes empresas cuenta con una política de seguridad y respaldo

86% de las empresas no estaría dispuesta a negociar el pago de un rescate

Fuente:
1.- Security Report, Latinoamerica 2024, ESET Latam

¿Cuáles son los roles más difíciles de cubrir en esta área? (Ejemplo: analistas SOC, ingenieros de redes, etc)

Ranking de dificultad en reclutamiento de posiciones:

1. **Cloud Security**
2. **Security Operation**
3. **Network Security**
4. **Software Developer Security**
5. **Risk Management**
6. **Security Assessment & Testing**
7. **Access Management**
8. **Compliance**

Fuentes:
1.- Cybersecurity: market data & análisis, STATISTA (octubre, 2023)
2.- Estudio Nacional de Ciberseguridad, Diario Financiero (Noviembre, 2023)

¿Cómo impacta la falta de personal en la detección y respuesta ante incidentes de red?

1. Intermitencias o pérdidas de servicios críticos
2. Aperturas de brechas de seguridad
3. Problemas en generación de respaldos por corrupción o pérdida de datos
4. Disminución de la confianza entre B2B y B2C
5. En caso de ciberataques graves se estima que las empresas pueden tener pérdidas que superan los 100 mil USD por evento

Microsoft proyecta que para el año 2025, habrá 3.5 millones de vacantes en el campo de la ciberseguridad a nivel mundial, lo que representa un impresionante aumento del 350% en un período de ocho años.

Además, actualmente por cada dos puestos de ciberseguridad ocupados, queda un tercero sin cubrir.

Región	Fuerza de Trabajo en Ciberseguridad	Incremento 2022-2023
América del Norte	1.495.825	11,30%
América Latina	1.285.505	4,50%
Europa	1.309.588	7,20%
Medio Este y África	401.582	11,70%
Asia Pacífico	960.231	11,80%

Fuente:
1.- Preocupa Falta de Talento en Ciberseguridad, cyber.lat

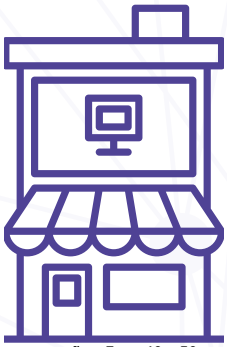
A pesar de las cifras de crecimiento el mercado no logra suplir las necesidades, estimándose un déficit de hasta un 30%.

Impacto de los fallos en la continuidad operacional

¿Cuánto cuesta a las empresas una caída de servicio en términos de productividad y pérdidas económicas?

Las caídas de servicio pueden tener un impacto significativo en la productividad y las pérdidas económicas de una empresa. Según datos de *ITIC y EN-Computers*, los costos por hora de inactividad varían dependiendo del tamaño de la empresa y la criticidad del servicio afectado.

Costo de una caída de servicio:



Empresas pequeñas: Entre 10 y 50 empleados
Entre 2.401 y 25.000 UF de ventas anuales

Costo por hora: $100,000 - $300,000
Costo por minuto: $1,670 - $5,000

Empresas medianas: Entre 51 y 199 empleados
Entre 25.000 y 100.000 UF de ventas anuales

Costo por hora: $301,000 - $1 millón
Costo por minuto: $5,017 - $16,700

Empresas grandes: Más de 200 empleados
Más de 100 UF de ventas anuales

Costo por hora: Hasta $10 millones
Costo por minuto: Hasta $166,667

Fuentes:
1.- Confiabilidad de servidores y aplicaciones en cifras: Entendiendo los "nueves", ITIC (Noviembre, 2022)
2.- ¿Cuál es el costo del tiempo de inactividad de TI para las pequeñas empresas en 2024?, Encomputers (2024)

Además, **la fiabilidad del sistema es clave** para reducir estos riesgos. Por ejemplo, un sistema con una disponibilidad del 99.9% (3 nueves) puede experimentar hasta 8.76 horas de inactividad al año, mientras que uno con 99.999% (5 nueves) se reduce a solo 5.26 minutos anuales. Empresas con infraestructuras críticas buscan alcanzar los seis o siete nueves para **minimizar el impacto económico**.

Las pérdidas no solo incluyen costos directos, sino también **impactos secundarios** como **pérdida de clientes, daños a la reputación y sanciones legales**. Según ITIC, más del 91% de las empresas encuestadas en 2022 consideraron que una hora de inactividad cuesta más de $300,000, y el 44% de ellas reportó pérdidas superiores a $1 millón por hora.

Para mitigar estos efectos, las empresas suelen **invertir en soluciones de alta disponibilidad y recuperación ante desastres**, pero esto conlleva costos adicionales en infraestructura y personal especializado.

Fiabilidad %	Tiempo de inactividad por año	Tiempo de inactividad por mes	Tiempo de inactividad por semana
90% (uno nueve)	36,5 días	72 horas	16,8 horas
95%	18,25 días	36 horas	8,4 horas
97%	10,96 días	21,6 horas	5,04 horas
98%	7,30 días	14,4 horas	3,36 horas
99% (dos nueves)	3,65 días	7,20 horas	1,68 horas
99,5%	1,83 días	3,60 horas	50,4 minutos
99,8%	17,52 horas	86,23 minutos	20,16 minutos
99,9% (tres nueves)	8,76 horas	43,8 minutos	10,1 minutos
99,95%	4,38 horas	21,56 minutos	5,04 minutos
99,99% (cuatro nueves)	52,56 minutos	4,32 minutos	1,01 minutos
99,999% (cinco nueves)	5,26 minutos	25,9 segundos	6,05 segundos
99,999999% (seis nueves)	31,5 segundos	2,59 segundos	0,605 segundos
99,9999999% (siete nueves)	3,15 segundos	0,259 segundos	0,0605 segundos

Fuente:
1.- Costo por hora del tiempo de inactividad Parte 2, ITIC (Septiembre 2024)

En el caso de diferentes países de la región, la pérdida monetaria es variable de acuerdo a diversas condiciones. A continuación revisaremos algunos casos específicos de distintos países sudamericanos y como enfrentan el impacto de los fallos en la continuidad operacional, además de como se ven afectados:

En el caso de Argentina, **cerca del 46% de empresas nacionales** declaran pérdidas anuales que varían entre **1 y 5 millones de dólares**, ocasionadas por fallos de software o problemas de mantención continua.

Respecto al riesgo de interrupción de servicios, un **80% de las empresas encuestadas declara estar expuesta**, mientras que la cifra en Latinoamérica es menor, cercana al **70%**, lo que indica una problemática a nivel país.

Fuente: Tricentis

En Perú, la continuidad operativa en Centros de Operaciones de Red (NOC) enfrenta riesgos significativos por la falta de automatización en la detección y respuesta ante incidentes. Durante 2024, el país registró más de un millón de incidentes informáticos y estudios regionales muestran que el **62% de las empresas** experimentó pérdida de datos sensibles, con costos que en Latinoamérica alcanzan en promedio **US 2,76 millones por filtración**.

Sin automatización, la gestión manual de alertas y escalamiento prolonga el tiempo de reacción y aumenta la probabilidad de interrupciones críticas en plataformas digitales, afectando operaciones y contratos. En contraste, las organizaciones que han incorporado automatización e inteligencia artificial en sus procesos de monitoreo reducen hasta en **83 días el ciclo de vida** de los incidentes, mitigando riesgos y evitando pérdidas financieras y reputacionales que, en escenarios extremos, **superan el millón de dólares**.

En **Experis Perú**, contamos con un NOC implementado en una de las empresas de Retail más grande del país, con monitoreo a más de **4,000 tiendas** a nivel nacional, un equipo de trabajo 2417, SLAs definidos e informes mensuales de servicio.

Fuente: Costo por hora del tiempo de inactividad Parte 2, ITIC (Septiembre 2024)

Brasil, por otra parte, **el 45% de las empresas encuestadas declararon haber enfrentado algún tipo de incidente de ciberseguridad**, en el último año (previo a la aplicación de la encuesta). El principal motivo de los fallos enfrentados fueron incidentes relacionados con gestión de crisis y continuidad de negocios y aceso no autorizado". Un **18%** de quienes respondieron la encuesta declaró perdidas superiores a **R$500**.

Fuente: Protiviti

Respecto a Colombia, las empresas del país enfrentan diariamente riesgos como el acceso no autorizado y el secuestro de información, la pérdida o daño de datos sensibles, ataques de hackers y la interrupción de sus plataformas digitales, debido a una gestión insuficiente o inadecuada de las inspecciones y controles en Tecnologías de la Información (TI). El **20% de empresas encuestadas** declaró haber enfrentado pérdidas de entre **250 USD a 3.600 USD**. El **15%** declaró haber sufrido pérdidas de entre **3.700 USD a 56.000 USD**. Finalmente, el **5%** declaró haber reportado pérdidas de hasta **960.000 USD**.

Fuente: Portafolio

¿Qué sectores son los más vulnerables?

Los sectores más vulnerables a las interrupciones de sistemas informáticos, como la reciente caída global de sistemas Microsoft, incluyen:

Aerolíneas y Aeropuertos: Graves retrasos y cancelaciones de vuelos. Aerolíneas como Ryanair, Vueling e Iberia tuvieron que recurrir a procedimientos manuales, generando largas colas y tiempos de espera prolongados. Fallos en sistemas de reserva y check-in, afectando la operación diaria de aeropuertos importantes.

Sector Bancario: Interrupciones en servicios de banca en línea, cajeros automáticos y plataformas de trading. Entidades como Kutxabank, VISA, Unicaja e Ibercaja reportaron problemas significativos. Afectó tanto a usuarios individuales como a operaciones comerciales.

Servicios Públicos y Hospitales: Disfunción en servicios esenciales, incluyendo hospitales y administraciones públicas. Interrupciones en operaciones diarias críticas.

Medios de Comunicación: Problemas técnicos, con ordenadores mostrando pantallazos azules, interrumpiendo las operaciones diarias.

Vertical	Costo promedio de tiempo de inactividad por hora
Banca/Finanzas	$10.3 Million (USD)
Gobierno	$8.5 Million
Alimentación / Hostelería	$7.9 Million
Salud	$9.2 Million
Manufactura	$9.1 Million
Media y Comunicaciones	$9.0 Million
Retail	$7.3 Million
Transporte	$7.2 Million
Servicios Públicos	$9.6 Million

Fuente:
1.- Costo por hora del tiempo de inactividad Parte 2, ITIC (Septiembre 2024)

Chile: ¿Tienen estrategias de mitigación o protocolos de respuesta a incidentes?

En Chile, las estrategias de mitigación y protocolos de respuesta a incidentes cibernéticos son cruciales para proteger la infraestructura digital. A continuación, se presentan algunas de las estrategias y protocolos implementados:

Estrategias de Mitigación y Protocolos de Respuesta:

1. Estrategia Nacional de Ciberseguridad:

Objetivos: Establecer un ciberespacio libre, abierto, seguro y resiliente. Incluye cinco ejes estratégicos: infraestructura, legislación, difusión, colaboración internacional y desarrollo de industria.

Medidas: Creación de la Agencia Nacional de Ciberseguridad (ANCI) para coordinar esfuerzos público-privados y fortalecer la resiliencia cibernética.

2. Implementación de Tecnologías Avanzadas:

Medidas: Uso de sistemas de detección y respuesta como FireEye, Splunk y CrowdStrike, que emplean análisis de comportamiento y machine learning para anticipar y neutralizar amenazas.

Tecnologías: Implementación de firewalls de próxima generación, sistemas de detección y prevención de intrusiones (IDS/IPS), y autenticación multifactor.

3. Capacitación y Cocienciación:

Programas: Educación en ciberseguridad para el personal sobre prácticas seguras, identificación de phishing y manejo seguro de datos confidenciales.

Campañas: Promoción de la concienciación ciudadana a través de campañas y foros.

4. Gestión de Incidentes:

Protocolos: Utilización de herramientas de gestión de incidentes y elaboración de informes post-incidente para mejorar la respuesta a ciber incidentes.

Colaboración: Coordinación entre el Ministerio del Interior y Seguridad Pública, CSIRT Nacional y sector privado para compartir información y responder a incidentes.

Colaboración: Coordinación entre el Ministerio del Interior y Seguridad Pública, CSIRT Nacional y sector privado para compartir información y responder a incidentes.

5. Legislación y Regulación:

Ley Marco de Ciberseguridad: Establece obligaciones para empresas privadas en cuanto a la notificación de incidentes significativos a la ANCI3.

Protección de Datos Personales: Regulaciones para proteger la privacidad y seguridad de los datos personales.

6. Auditorías y Actualizaciones:

Auditorías: Realización periódica de auditorías de seguridad para identificar vulnerabilidades y cumplir con estándares internacionales.

Actualizaciones: Mantenimiento regular de sistemas y software para parchar vulnerabilidades conocidas.

Fuente:
1-Estrategia nacional de ciberseguridad, Ministerio del interior y seguridad pública. (2023)
2-Cibercrimen en 2025: Amenazas en aumento y estrategias para proteger tu empresa, Entel digital (2025)

Perú: ¿Tienen estrategias de mitigación o protocolos de respuesta a incidentes?

En Perú, las empresas están adoptando estrategias de mitigación y protocolos de respuesta a incidentes para enfrentar caídas de servicio y amenazas cibernéticas.

Estrategias de Mitigación y Protocolos de Respuesta:

1. Guía para la Conformación e Implementación del Equipo de Respuestas ante Incidentes de Seguridad Digital:

Medidas: Establece lineamientos para que entidades públicas y privadas conformen equipos de respuesta ante incidentes (CSIRT), incluyendo detección, contención, recuperación y análisis post-incidente.

2. Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad – Resolución SBS N.º 504-2021

Medidas: Obliga a las entidades financieras a implementar un Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C), con protocolos de prevención, detección, respuesta y recuperación.

3. Procedimiento para la Gestión de Incidentes de Seguridad de la Información

Medidas: Documento técnico que describe cómo gestionar incidentes dentro de un Sistema de Gestión de Seguridad de la Información (SGSI), aplicable a empresas del sector telecomunicaciones y TI.

Fuente:
1-Centro nacional de seguridad digital – Guía para la conformación e implementación del equipo de respuestas ante incidentes de seguridad digital (2024)
2-Superintendencia de banca, seguros y AFP – SBS (2021)

Colombia: ¿Tienen estrategias de mitigación o protocolos de respuesta a incidentes?

En el caso de Colombia, existen estrategias y protocolos bien definidos para la gestión de incidentes de seguridad digital, tanto en el sector público como en el privado.

Estrategias de Mitigación y Protocolos de Respuesta:

1. ColCERT – Equipo Nacional de Respuesta a Incidentes

Medidas: Desarrolla y divulga protocolos, guías y recomendaciones para la gestión de incidentes, y promueve la creación de CSIRT sectoriales (equipos de respuesta a incidentes en sectores específicos).

1. Guía del MinTIC para la Gestión de Incidentes

Medidas: El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) publicó una guía que establece las fases del ciclo de vida de la gestión de incidentes:

- Preparación
- Detección y análisis
- Contención, erradicación y recuperación
- Lecciones aprendidas

¿Qué porcentaje de incidentes de red o caídas de sistemas afectan la productividad?

El porcentaje de incidentes de red o caídas de sistemas que afectan la productividad varía según la industria y la infraestructura tecnológica de cada empresa. Según un informe de IDC, las caídas de servicio pueden reducir la productividad hasta en un **40%**, dependiendo del tipo de interrupción y la rapidez con la que se restablezca el servicio. Empresas con infraestructuras críticas, como centros de datos y telecomunicaciones, suelen experimentar un impacto más significativo debido a la dependencia de sistemas siempre operativos.

Fuente:
1-Colombian Computer Emergency Response Team (2025)
2-Guía de apoyo para el Procedimiento Gestión de Incidentes de Seguridad de la Información. (2022)

Uruguay: ¿Tienen estrategias de mitigación o protocolos de respuesta a incidentes?

Finalmente, Uruguay posee estrategias nacionales y protocolos específicos para la mitigación de riesgos y respuesta a incidentes de ciberseguridad, tanto en el sector público como en el privado. Estas iniciativas están lideradas por organismos como CERTuy y Agesic, y se alinean con estándares internacionales.

Estrategias de Mitigación y Protocolos de Respuesta:

1. Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)

Medidas: Es el equipo oficial de respuesta a incidentes del país. Ofrece:

- Guías de buenas prácticas
- Alertas de amenazas
- Protocolos de reporte y gestión de incidentes
- Autoevaluaciones de ciberseguridad

2. Estrategia Nacional de Ciberseguridad del Uruguay 2024–2030

Medidas: Documento marco que establece:

- Protocolos de respuesta a incidentes
- Protección de infraestructuras críticas
- Fortalecimiento de capacidades técnicas
- Participación del sector privado y académico

Fuente:
1- CERTuy –Gub.Uy (2025)
2-Estrategia Nacional de Ciberseguridad – Agesic (2024)

Ciberseguridad y Amenazas Emergentes

¿Qué tan preparadas están las empresas para responder a ataques cibernéticos?

Las empresas en **Chile** enfrentan varios desafíos en su preparación para detectar y responder a ataques cibernéticos. A continuación, se presentan los principales retos y el nivel de preparación actual: **Desafíos Clave**

Conocimiento y Cumplimiento Normativo: Más del 55% de los directores en Chile no está al tanto de los riesgos regulatorios en ciberseguridad, lo que pone en riesgo el cumplimiento de las nuevas leyes, como la **Ley Marco de Ciberseguridad** (21.663) y la futura Ley 21.719 sobre Protección de Datos Personales.

En **Brasil**, un estudio realizado por la empresa de ciberseguridad ***Vultus Cybersecurity Ecosystem*** reveló que el 67% de las compañías carecen de procesos establecidos para la protección digital, mientras que el **55% nunca ha implementado un monitoreo continuo de amenazas**. Además, el informe señala que el **80% de las organizaciones no dispone de un plan integral para responder a ciberataques**, lo que evidencia la alta vulnerabilidad de las empresas brasileñas frente a ataques informáticos y filtraciones de datos.

Fuente: 1-Tres desafíos clave para los directorios en Chile en torno a ciberseguridad este 2025, Forbes Chile (Febrero 2025)
2-El 80% de las empresas brasileñas no tienen un plan de respuesta a ciberataques – SitePD (2025)

En **Argentina**, según un estudio global de **Cisco** que incluye a empresas del país, **solo el 4% de las organizaciones alcanza un nivel "maduro" de preparación para enfrentar amenazas cibernéticas**, reflejando una mejora mínima respecto al año anterior y evidenciando que la mayoría aún no cuenta con capacidades robustas para protegerse eficazmente. Esta baja preparación es especialmente crítica en las pymes, que son blanco frecuente de ataques debido a su limitada infraestructura tecnológica y recursos para seguridad

Las empresas **peruanas** enfrentan un promedio de más de **1,300 ciberataques cada semana**, lo que evidencia la magnitud del riesgo al que están expuestas. Sin embargo, la mayoría carece de estrategias integrales de prevención y solo un reducido número, **menos de 100 organizaciones, ha contratado seguros contra riesgos cibernéticos, lo que refleja una alta vulnerabilidad ante estas amenazas**.

Fuente:
1.- 2025 Cisco Cybersecurity Readiness Index (2025)
2. Empresas peruanas bajo asedio – America retail (2025)

Nivel de Preparación Actual:

Conciencia y Planificación: Aunque hay una creciente conciencia sobre la importancia de la ciberseguridad, muchos directores carecen de conocimiento detallado sobre los riesgos y regulaciones.

Implementación de Tecnologías: Las empresas están adoptando tecnologías de detección y respuesta, pero la efectividad depende de la inversión y la gestión adecuada.

Gobernanza y Cultura de Seguridad: La ciberseguridad debe ser parte de las decisiones clave y de la cultura organizacional. En Chile, las empresas avanzan en su preparación ante ciberataques, aunque aún enfrentan retos en regulación, inversión y gobernanza.

Insights y Perfiles Recomendados

Zero Trust la gestión de riesgos de terceros y el marco de gobernanza de las empresas son las prioridades de inversión.

40% de las empresas cree que la falta de personal es una barrera fundamental. Seguido del marco regulatorio y seguridad de datos por terciarización.

63% de las organizaciones considera que sus presupuestos en redes y ciberseguridad es deficiente.

86% de las empresas no está dispuesta a negociar un rescate de información.

Cloud Security, Security Operation y Network Security son de alta demanda no cubierta.

Los costos de una caída de servicio varían de acuerdo a la duración de este y al tamaño de la empresa, pero estos pueden ir desde **$100.000 USD por hora en pequeñas empresas** hasta **$10.000.000 USD por hora en grandes empresas**.

Más del **91%** de las empresas encuestadas en **2022** consideraron que una hora de inactividad cuesta más de **$300,000 USD**, y el **44%** de ellas reportó pérdidas superiores a **$1 millón USD por hora**.

Más del **55%** de los directores en Chile no está al tanto de los riesgos regulatorios en ciberseguridad, lo que pone en riesgo el cumplimiento de las nuevas leyes, como la **Ley Marco de Ciberseguridad (21.663)** y la futura **Ley 21.719** sobre Protección de Datos Personales.

Solo el 50% de los directorios asigna un presupuesto mínimo a ciberseguridad, lo que limita su capacidad de respuesta ante incidentes.

Perfiles más recomendados

De acuerdo a lo abordado en el informe, los siguientes perfiles son los más solicitados por el mercado en la actualidad, en centros de operaciones de red.

Ingeniero NOC Senior con Especialización en Redes IP/MPLS:

Puesto: Ingeniero NOC Senior (Redes IP/MPLS)
Funciones:

- Monitorear redes backbone y de acceso mediante herramientas NMS (como SolarWinds, Zabbix, o Nagios).
- Gestionar incidentes de alta prioridad (P1/P2), liderando su resolución y análisis post-mortem.
- Configurar y mantener equipos de red en entornos IP/MPLS.
- Automatizar tareas de monitoreo usando scripts (Python, Bash).
- Coordinar con equipos de ingeniería, soporte y proveedores para asegurar continuidad de servicio.

Estudios: Ingeniería en Telecomunicaciones, Electrónica, Redes o afines.
Certificaciones deseables: CCNP, JNCIS, ITIL Foundations.
Experiencia: Mínimo 5 años en NOC, con dominio de protocolos de enrutamiento (BGP, OSPF, MPLS).
Expectativa salarial: USD $3.500 – $4.000

Especialista Senior en Detección y Gestión de Incidentes de Red

Puesto: Especialista Senior en Incidentes de Red (NOC/SOC)
Funciones:

- Identificar patrones de degradación del servicio o fallos críticos mediante herramientas de correlación de eventos (Splunk, Elastic, IBM QRadar).
- Supervisar redes multiservicio (voz, datos, video) 24x7 para clientes corporativos y servicios críticos.
- Generar reportes ejecutivos de disponibilidad y performance.
- Coordinar el proceso completo de incident response, desde detección hasta cierre.
- Colaborar estrechamente con equipos SOC para detectar posibles amenazas cruzadas en red.

Estudios: Ingeniería Informática, Telecomunicaciones o afines.
Certificaciones deseables: ITIL v4, CompTIA Network+, Cisco ENCOR.
Experiencia: 6 años en operación de redes o centros NOC/SOC híbridos.
Expectativa salarial: USD $3.200 – $3.800

Referencias:

- Server and Application Reliability by the Numbers: Understanding “The Nines” – Information Technology Intelligence Consulting
- ITIC 2024 Costo por hora de inactividad (Parte 2) – Consultoría de inteligencia en tecnologías de la información
- What is the cost of IT downtime for small businesses in 2024?
- Caída Global de Sistemas Microsoft: Aeropuertos, Bancos y Servicios Públicos Severamente Afectados – T I B O X
- 3 pasos para una efectiva mitigación de riesgos cibernéticos
- Ciberseguridad en Chile: Más allá de las amenazas, una estrategia de protección - Insurtechile
- Ciberseguridad en Chile, estrategias para fortalecer las defensas digitales - AmericaMalls & Retail
- Desafios-Legales-y-Estrategia-de-Cibserseguridad-Municipal.pdf
- Ciberseguridad industrial en Chile: retos y estrategias para empresas
- Cibercrimen en 2025: Amenazas en aumento y estrategias para proteger tu empresa
- The Cost of Downtime in Datacenters and the Preventative Measures to Alleviate
- Tres desafíos clave para los directorios en Chile en torno a ciberseguridad este 2025 - Forbes Chile
- Em um ano, 70% das indústrias do país registraram ao menos um episódio de queda de energia, diz CNI
- Dois terços das indústrias têm prejuízos com falhas no fornecimento de energia elétrica, diz pesquisa da CNI
- Um panorama sobre como as empresas brasileiras lidam com a Gestão de Crises e a Continuidade de negócios.
- Hay empresas que pierden hasta $4.000 millones por ciberataques
- Superintendencia de banca y seguros Perú
- Guía para la Conformación e Implementación del Equipo de Respuestas ante Incidentes de Seguridad Digital
- PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD
- Colcert GOV CO
- Guía de apoyo para el Procedimiento Gestión
- Centro nacional de respuesta a incidentes de seguridad informática
- Empresas peruanas bajo asedio: Más de 9 millones de ciberataques en un año - AmericaMalls & Retail

- El 62% de los ciberataques en Perú en 2025 comenzó con campañas de phishing - Rumbo Económico
- Cybersecurity Readiness Index 2025
- Ataques cibernéticos y logística en riesgo: la nueva amenaza para la cadena de suministro - Infobae
- Los ataques cibernéticos ya son la principal preocupación en una de cada dos empresas y en Argentina persiste la falta de preparación para evitarlos – Argencon
- Cámara de comercio de lima
- IBM Latin America Newsroom


Experis®
ManpowerGroup