WEBINAR GRATUITO

CHRYSALIS
Cyber Shield Intelligence

RETOS DE CIBERSEGURIDAD 2025

Construyendo una hoja de ruta cibersegura para la empresa

- Conoce el Panorama actual de ciberseguridad.
- Principales retos de ciberseguridad actuales y para 2025.
- Como construir una hoja de ruta cibersegura para tu negocio.

EXPOSITOR

LEONEL MARÍN RAMIREZ

CONSULTOR SENIOR DE CIBERSEGURIDAD - DOCENTE EN POSTGRADOS DE CIBERSEGURIDAD

FECHA: MIERCOLES 4 DE DICIEMBRE DE 2024 **HORA: 11:00 AM**

LEONEL MARIN RAMIREZ

Formación académica:
- Ingeniero informático
- Especialista en Seguridad Informática
- Especialista en Gerencia de Proyectos
- Magíster en Dirección y Administración de Empresas

Práctica profesional:
- 13 años de experiencia en Seguridad y Ciberseguridad.
- Consultor Independiente de Ciberseguridad y fundador de **CHRYSALIS**
- Líder de Ciberseguridad en XM S.A. e ingeniero de seguridad en organizaciones como Grupo EPM, Grupo Éxito.

Participación en otras organizaciones:
- Comité de Ciberseguridad del CNO

Agenda

1. Panorama Actual de Ciberseguridad
2. Principales Retos 2025
3. Hoja de Ruta Cibersegura
4. Preguntas y Respuestas

Agenda

1. **Panorama Actual de Ciberseguridad**
2. Principales Retos 2025
3. Hoja de Ruta Cibersegura
4. Preguntas y Respuestas

1. Panorama actual de ciberseguridad

El cibercrimen continúa evolucionando

1. Las organizaciones y las personas enfrentan amenazas sofisticadas y persistentes, originadas en actores con capacidades avanzadas

2. Las tácticas de los atacantes evolucionan para ser más sigilosas y enfocadas a puntos críticos

1. Panorama actual de ciberseguridad

https://www.itdigitalsecurity.es/itdigitalsecurity/2024/10/el-43-de-los-ciberataques-se-dirigen-a-las-pyme-que-no-estan-preparadas-para-mitigarlos-marco-fruehauf-grenke

1. Panorama actual de ciberseguridad

Cifras clave

USD $1 Millón

Costo de rescatar los datos después de un ciberataque. [1]

197 días

Es el tiempo promedio para identificar una brecha de datos. [2]

60% de Pymes

Cierran después de 6 meses de sufrir un ciberataque debido al precio que deben pagar por recuperarse. [3]

[1] https://www.portafolio.co/tecnologia/costos-para-recuperar-informacion-secuestrada-en-un-ciberataque-589230
[2] https://www.netwrix.es/threat_detection_software.html
[3[] https://blog.camelsecure.com/60-de-pymes-colapsan-6-meses-despu%C3%A9s-de-un-ciberataque

1. Panorama actual de ciberseguridad

Principales amenazas

- Ransomware como Servicio (RaaS)
- Spear Phishing
- Compromisos de Correo Empresarial
- Ataques a la Cadena de Suministro

1. Panorama actual de ciberseguridad

Ransomware como servicio (RaaS)

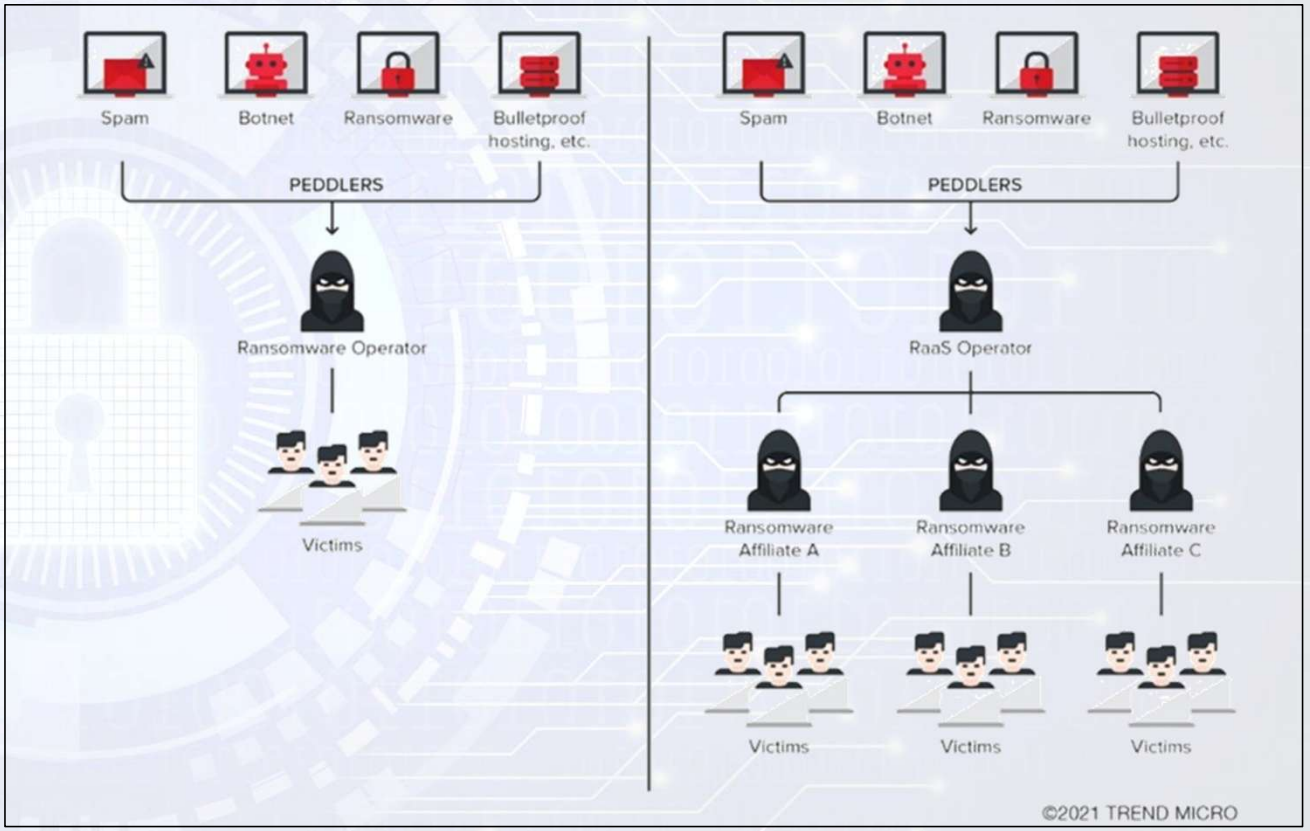
El ransomware como servicio (RaaS) es un modelo de negocio que implica vender o alquilar ransomware a compradores, llamados afiliados.

Se puede atribuir a RaaS el mérito de ser una de las principales razones de la rápida proliferación de ataques de ransomware, ya que ha facilitado que una variedad de actores de amenazas, incluso aquellos que tienen poco conocimiento técnico, implementen ransomware contra sus objetivos.

https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas

1. Panorama actual de ciberseguridad

Comparación de operaciones directas de ransomware (izquierda) y operadores de RaaS (derecha)



1. Panorama actual de ciberseguridad

Ransomware como servicio (RaaS)

	Semestre 1 2023	Semestre 2 2023
Total de grupos activos de RaaS y relacionados con RaaS	45	52
Total de victimas	1,999	2524

Número de grupos de extorsión y RaaS activos y organizaciones víctimas de ataques de ransomware exitosos en 2023

https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/rise-in-active-raas-groups-parallel-growing-victim-counts-ransomware-in-2h-2023

1. Panorama actual de ciberseguridad

Ransomware como servicio (RaaS)

Fuente: SOPHOS: El estado del ransomware 2023. Resultados de una encuesta independiente a 3000 responsables de TI/Ciberseguridad en 14 países.

1. Panorama actual de ciberseguridad

Spear Phishing: Características

- **Ataques personalizados**: Los atacantes investigan a sus víctimas para recopilar información relevante, como nombres, cargos y relaciones laborales, lo que les permite crear mensajes que parecen legítimos y relevantes
- **Métodos de Contacto**: Usualmente, el phishing dirigido se lleva a cabo a través de correos electrónicos que imitan a fuentes confiables. Estos mensajes pueden incluir enlaces a sitios web falsos o archivos adjuntos infectados con malware.
- **Objetivos Específicos:** Los atacantes pueden dirigirse a ejecutivos de alto nivel (un ataque conocido como whaling) o a empleados en departamentos críticos como finanzas, buscando obtener credenciales o realizar transferencias de dinero fraudulentas

Factor humano como vector principal

1. Panorama actual de ciberseguridad

Spear Phishing

Técnicas comunes	Prevención y protección
Suplantación de Identidad	Formación continua
Enlaces Maliciosos	Simulaciones de Phishing
Archivos Adjuntos Infectados	Políticas de seguridad rigurosas

1. Panorama actual de ciberseguridad

Spear Phishing

https://www.europol.europa.eu/media-press/newsroom/news/criminal-phishing-network-resulting-in-over-480-000-victims-worldwide-busted-in-spain-and-latin-america

1. Panorama actual de ciberseguridad

Spear Phishing

Los investigadores informaron de 483.000 víctimas en todo el mundo que intentaron recuperar el acceso a sus teléfonos y fueron víctimas de phishing en el proceso. Las víctimas son principalmente ciudadanos hispanohablantes de países europeos, norteamericanos y sudamericanos.

La exitosa operación se llevó a cabo gracias a la cooperación internacional entre autoridades policiales y judiciales de España, Argentina, Chile, Colombia, Ecuador y Perú.

La semana de acción tuvo lugar entre el 10 y el 17 de septiembre y se saldó con 17 detenciones, 28 registros y 921 artículos incautados, principalmente teléfonos móviles pero también otros dispositivos electrónicos, vehículos y armas.

1. Panorama actual de ciberseguridad

Compromiso de correo empresarial (BEC)

- **Ataque dirigido que suplanta identidades legítimas.**
- **Objetivo:** Obtener acceso o realizar transferencias fraudulentas
- **Altamente efectivo: L**os ataques BEC son considerados uno de los métodos más lucrativos para el fraude, resultando en pérdidas significativas para las empresas.
- **Pérdidas reportadas: $2.7B en 2022 (FBI IC3) [1]**: Este monto representa más del 27% del total de pérdidas por delitos cibernéticos, según el FBI Internet Crime Complaint Center (IC3)

[1] https://abnormalsecurity.com/blog/2022-fbi-ic3-report

1. Panorama actual de ciberseguridad

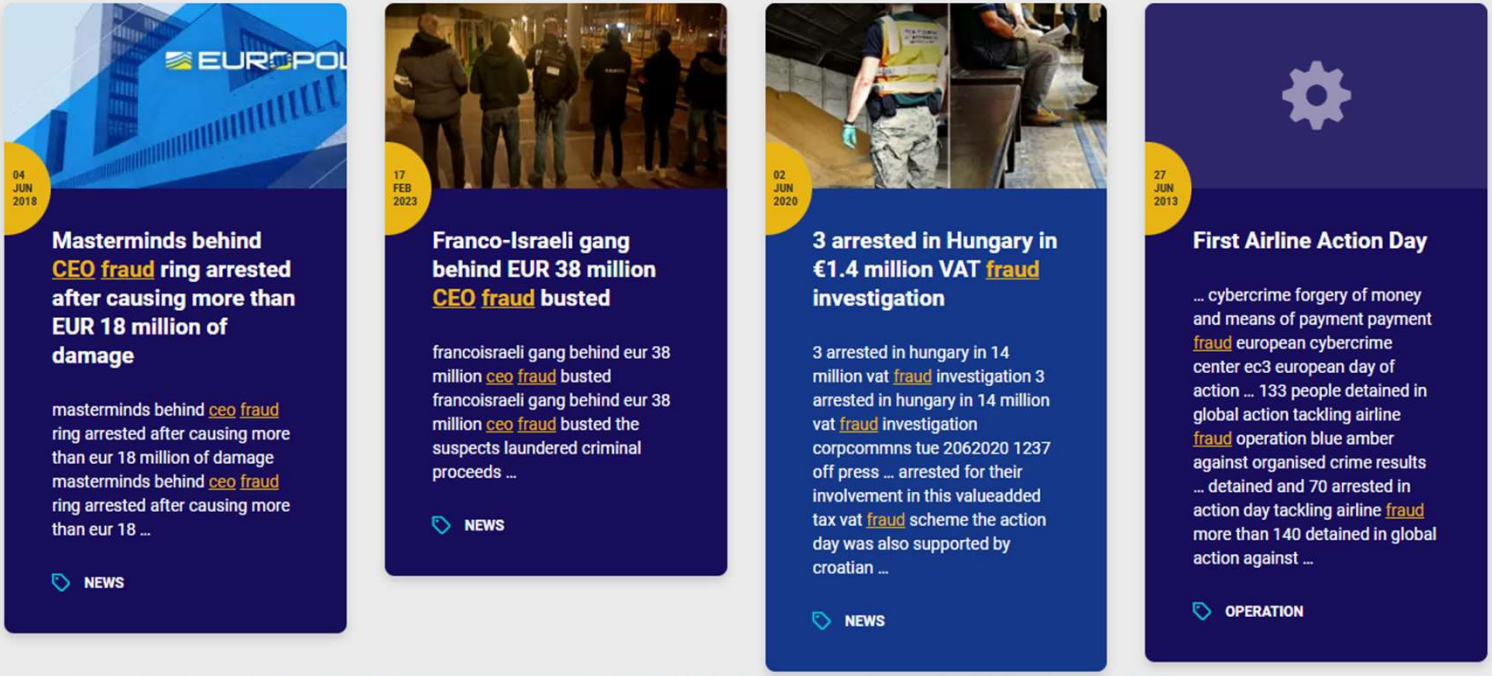
Compromiso de correo empresarial (BEC)

Principales variantes

- Suplantación de CEO/Ejecutivos (Fraude del CEO)
- Compromiso de Cuentas de Proveedores
- Compromiso de cuenta de correo empresarial

1. Panorama actual de ciberseguridad

Compromiso de correo empresarial (BEC)



https://www.europol.europa.eu/search?q=CEO%20fraud&sort=relevance

1. Panorama actual de ciberseguridad

Compromiso de correo empresarial (BEC)

Con el apoyo de 257 bancos y socios del sector privado, se denunciaron 1.719 transacciones de mulas de dinero, con pérdidas totales que ascendieron a casi 31 millones de euros. Entre esas transacciones de mulas de dinero, más del 90% estaban vinculadas a delitos cibernéticos, como phishing, fraude en subastas en línea, Business Email Compromise (BEC) y fraude de directores ejecutivos . Por primera vez, las autoridades policiales denunciaron estafas románticas y fraudes de vacaciones (fraude en reservas). Además, se identificó un papel cada vez mayor de las transacciones de criptomonedas (Bitcoin) en los esquemas de lavado de dinero utilizados por los delincuentes.

https://www.europol.europa.eu/media-press/newsroom/news/159-arrests-and-766-money-mules-identified-in-global-action-week-against-money-muling

1. Panorama actual de ciberseguridad

Compromiso de correo empresarial (BEC)

Estrategias de mitigación

Controles técnicos	Controles Administrativos
SPF, DKIM, DMARC	Verificación fuera de banda
Autenticación multifactor	Procesos de aprobación dual
Filtrado de correo avanzado	Listas blancas de proveedores

1. Panorama actual de ciberseguridad

Ataques a la cadena de suministro

Características

- Compromiso a través de proveedores y terceros
- Explotación de confianza establecida
- Afectación en cascada
- Impacto multiplicado

1. Panorama actual de ciberseguridad

Ataques a la cadena de suministro

Impacto en números:

62% de los ataques a proveedores afectan a empresas medianas

$1.4M costo promedio por incidente

430% incremento en ataques (2020-2022)

287 días promedio de detección

Fuente: BlueVoyant Supply Chain Defense Report 2023. https://www.bluevoyant.com/blog/the-state-of-supply-chain-defense-in-2023

1. Panorama actual de ciberseguridad

Ataques a la cadena de suministro: Tipos de ataques

Compromiso de software

- Código malicioso en actualizaciones
- Librerías comprometidas
- Backdoors en aplicaciones

Caso SolarWinds (2020)

- **Tipo:** Malware insertado en actualizaciones legítimas
- Vector: Los atacantes comprometieron el sistema de desarrollo de software
- **Impacto:** Más de 18,000 organizaciones instalaron el software malicioso
- **Método:** El malware SUNBURST se distribuyó a través de actualizaciones oficiales
- **Tiempo sin detectar:** Más de 9 meses

1. Panorama actual de ciberseguridad

Ataques a la cadena de suministro: Tipos de ataques

Compromiso de hardware

- Dispositivos alterados
- Firmware modificado
- Componentes falsificados

Caso Supermicro (2018)

- **Tipo:** Manipulación de placas base durante la fabricación
- **Vector:** Inserción de chips espía en la cadena de montaje
- **Impacto:** Servidores comprometidos en múltiples empresas
- **Método:** Chips diminutos añadidos a las placas base
- **Consecuencia**: Capacidad de acceso remoto no autorizado

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=2018-the-big-hack

1. Panorama actual de ciberseguridad

Ataques a la cadena de suministro: Tipos de ataques

Compromiso de servicios

- Accesos de proveedores
- Credenciales comprometidas
- Servicios en la nube

Caso Target (2013)

- **Tipo:** Compromiso a través de proveedor de HVAC (Calefacción, Ventilación y Aire Acondicionado)
- **Vector:** Credenciales robadas de un proveedor de servicios
- **Impacto:** 40 millones de tarjetas de crédito comprometidas
- **Método:** Uso de accesos legítimos del proveedor
- **Costo:** Más de $200 millones

https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

1. Panorama actual de ciberseguridad

Diagnóstico de riesgos de terceros

- Identificación y clasificación del proveedor
- Evaluación de seguridad del proveedor
- Evaluación de riesgos operativos
- Evaluación y cumplimiento legal y contractual
- Evaluación de la cadena de suministro
- Gestión continua y reevaluación
- Calificación final de riesgo y decisión

https://chrysalis.com.co/herramienta-de-diagnostico-de-riesgos-de-terceros-protege-tu-empresa-en-7-pasos-clave/

Agenda

1. Panorama Actual de Ciberseguridad
2. **Principales Retos 2025**
3. Hoja de Ruta Cibersegura
4. Preguntas y Respuestas

2. Principales retos de ciberseguridad 2025

El Panorama está cambiando

Lo que vemos hoy:

- Más empleados trabajando desde casa
- Servicios moviéndose a la nube
- Ataques más sofisticados, pero más baratos
- Clientes preocupados por su información

¿Por qué es importante?

- Los ataques son cada vez más frecuentes
- Las empresas medianas son el nuevo objetivo
- La recuperación es costosa y difícil
- Los clientes exigen más seguridad

2. Principales retos de ciberseguridad 2025

Datos que nos preocupan

Situación actual

- 1 de cada 3 sufrirá un ataque
- 60% no sobrevive 6 meses después
- 3 semanas promedio de interrupción

La buena noticia

- La mayoría de los ataques son prevenibles
- Hay soluciones accesibles
- No necesitas ser experto
- Podemos empezar con pasos simples

2. Principales retos de ciberseguridad 2025

¿Y si nos hacemos las preguntas clave?

Superficie de ataque

Postura de ciberseguridad

¿Qué tan expuestos estamos frente a ciberataques?

Explotabilidad de vulnerabilidades

Madurez en la gestión de la ciberseguridad

2. Principales retos de ciberseguridad 2025

¿Y si nos hacemos las preguntas clave?

Bajo nivel de aseguramiento de controles

Fallas en el software

¿Cuál es la probabilidad de que tengamos un ciberataque exitoso?

Accesos no estandarizados ni monitoreados

Acelerada digitalización

2. Principales retos de ciberseguridad 2025

¿Y si nos hacemos las preguntas clave?

Anticipación

Resiliencia

¿Qué tan rápido nos podemos recuperar de un ciberataque exitoso?

Aprendizaje

2. Principales retos de ciberseguridad 2025

	Retos	Problemas comunes	Soluciones prácticas
Retos técnicos	Gestión de la superficie de ataque	• Dispositivos conectados sin control • Aplicaciones en la nube sin visibilidad. • accesos remotos no seguros	• Inventario de activos de información. • Segmentación de red • Gestión de accesos e identidades.
	Evaluación de controles	• Controles desactualizados. • Falta de monitoreo. • Falta de documentación y evidencias de ejecución del control	• Medición periódica de efectividad de los controles. • Comenzar por lo básico. • Ajustar según resultados
	Gestión de vulnerabilidades	• Obsolescencia tecnológica. • Software no soportado. • Parches sin aplicar	• Inventario de software. • Análisis de riesgos de las vulnerabilidades. • Controles compensatorios.

2. Principales retos de ciberseguridad 2025

	Retos	Problemas comunes	Soluciones prácticas
Retos organizacionales	Mejorar el nivel de madurez de ciberseguridad	• Procesos informales. • Roles no definidos. • Métricas limitadas.	• Evaluación periódica. • Definir roles clave. • Implementar métricas.

	Gobernanza de ciberseguridad	• Falta de visibilidad
		• Decisiones reactivas y no proactivas
		• Prioridades confusas
			• Definir una gobernanza básica
			  • Comité de ciberseguridad
			  • Roles y responsabilidades.
			  • Reportes periódicos.

	Digitalización	• Adopción acelerada. • Nuevos riesgos sin análisis. • Cambio constante	• Evaluación de riesgos • Monitoreo continuo • Gestión del cambio

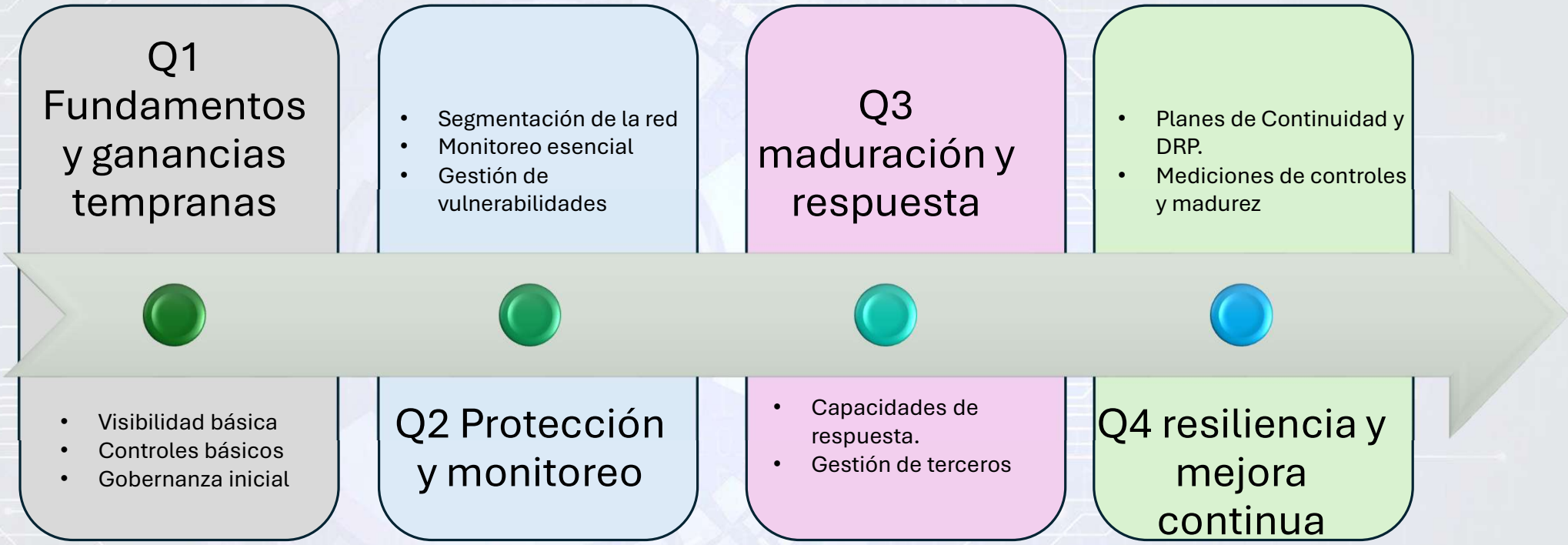
2. Principales retos de ciberseguridad 2025

	Retos	Problemas comunes	Soluciones prácticas
Retos operativos	Recuperación ante desastres	• Tiempos de recuperación. • Falta definición de los RTO/RPO • Respaldos corruptos o incompletos. • Dependencias no identificadas	• Respaldos basados en criticidad. • Procedimientos documentados. • Pruebas de recuperación
	Detección y respuesta de incidentes	• Falta de monitoreo 24/7 • Tiempo de respuesta lento • Coordinación deficiente entre las áreas.	• Sistemas de gestión de logs (SIEM) • Implementación SOAR • Identificación de amenazas (CTI) • Realizar simulacros y TTX
	Gestión de terceros y cadena de suministro	• Accesos no controlados. • Proliferación de proveedores. • Dependencias críticas no identificadas.	• Evaluación de proveedores • Gestión de accesos y conexiones. • Monitoreo continuo. • Gestión de acuerdos y contratos.

Agenda

1. Panorama Actual de Ciberseguridad
2. Principales Retos 2025
3. **Hoja de Ruta Cibersegura**
4. Preguntas y Respuestas

3. Hoja de ruta cibersegura 2025



1.Documentar mejoras

3. Hoja de ruta cibersegura 2025

Consideraciones de implementación

1. Priorización	2. recursos	3. Medición
Enfocarse en riesgos críticos primero	Aprovechar herramientas existentes	Establecer métricas desde el inicio
Implementar controles básicos antes que avanzados	Utilizar soluciones open source cuando sea posible	Medir progreso regularmente
Asegurar quick wins en cada fase	Considerar servicios gestionados (CISOaaS)	Ajustar según resultados
Balancear esfuerzo y beneficio	Rentabilizar inversiones	Documentar mejoras

3. Hoja de ruta cibersegura 2025

En Chrysalis tenemos un equipo experto en ciberseguridad que le va a ayudar en:

- Rentabilizar sus inversiones en ciberseguridad y disminuir los riesgos.
- Mejorar el nivel de madurez en ciberseguridad
- Fortalecer las capacidades de detección y respuesta de incidentes

CHRYSALIS
Cyber Shield Intelligence

Construir una hoja de ruta cibersegura para su empresa!!

Agenda

1. Panorama Actual de Ciberseguridad
2. Principales Retos 2025
3. Hoja de Ruta Cibersegura
4. **Preguntas y Respuestas**

Muchas gracias!!

www.chrysalis.com.co

comercial@chrysalis.com.co

+57 304 3368256

https://chrysalis.com.co/libro/