Plan Ejecutivo de Respuesta a Incidentes de Ransomware

Empresa: TechCo
Marco de referencia: NIST Cybersecurity Framework (CSF)
Control del Documento
Cuadro de Versiones

Versión	Fecha	Descripción del Cambio	Autor
1.0	2025-12	Versión inicial del Plan de Respuesta a Incidentes de Ransomware	CISO / Seguridad de la Información

Aprobaciones y Responsabilidades

Rol	Nombre / Área	Fecha	Firma
Elaboró	CISO / Seguridad de la Información		
Revisó	Comité de Seguridad / Riesgos		
Autorizó	Alta Dirección / Dirección General		

1. Resumen Ejecutivo

TechCo, empresa dedicada a la provisión de servicios en la nube y a la gestión de información sensible d**e clientes, ha sufrido un incidente grave de ransomware que impactó directamente la disponibilidad, integridad y confidencialidad de sus activos críticos. El ataque tuvo su origen en una campaña de phishing dirigida a un empleado, lo que p**ermitió la ejecución de malware y su posterior propagación lateral dentro de la red corporativa.

El presente documento desarrolla un **Plan de Respuesta a Incidentes de Ransomware**, alineado con el **NIST Cybersecurity Framework (CSF)**, con un enfoque ejecutivo y estratégico. Su objetivo es fortalecer la postura de ciberseguridad de TechCo, reducir la probabilidad de incidentes futuros y minimizar el impacto operativo, financiero, legal y reputacional ante ataques similares.

2. Alcance y Objetivos del Plan

2.1 Alcance

El presente plan de respuesta a incidentes de ransomware aplica de manera integral a toda la organización TechCo y cubre los activos, procesos y recursos que resultan críticos para la continuidad del negocio y la protección de la información.

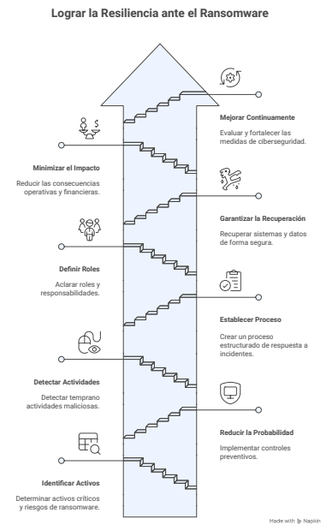
- Todos los sistemas de información de TechCo, tanto en entornos **on-premise** como en infraestructuras y servicios **cloud**.
- Datos de usuarios, empleados y socios comerciales, con especial énfasis en información personal, financiera y confidencial.
- Infraestructura tecnológica, incluyendo servidores, estaciones de trabajo, redes, plataformas de virtualización y servicios de respaldo.
- Procesos operativos y de negocio que dependen de la disponibilidad y confiabilidad de los sistemas de información.
- Personal interno, proveedores y terceros que cuenten con acceso lógico o físico a los sistemas y datos de TechCo.

El plan se orienta específicamente a incidentes de ransomware, sin perjuicio de que muchos de los controles, procedimientos y capacidades aquí definidos puedan ser reutilizados para la gestión de otros tipos de incidentes de ciberseguridad.

2.2 Objetivos

Los objetivos del presente Plan de Respuesta a Incidentes de Ransomware son los siguientes:

- Identificar y clasificar los activos de información críticos de TechCo, así como los riesgos de ransomware que pueden afectar su confidencialidad, integridad y disponibilidad.
- Reducir la probabilidad de ocurrencia de ataques de ransomware mediante la implementación de controles preventivos técnicos, organizativos y de concientización del personal.
- Detectar de manera temprana actividades maliciosas asociadas a ransomware, minimizando el tiempo de permanencia del atacante dentro del entorno tecnológico.
- Establecer un proceso estructurado y coordinado de respuesta a incidentes que permita contener, erradicar y gestionar eficazmente un ataque de ransomware.
- Definir roles, responsabilidades y canales de comunicación claros para garantizar una toma de decisiones oportuna y alineada con los objetivos del negocio.
- Garantizar la recuperación segura y priorizada de los sistemas y datos afectados, asegurando la continuidad del negocio y la prestación de servicios críticos.
- Minimizar el impacto operativo, financiero, legal y reputacional derivado de un incidente de ransomware.
- Incorporar un enfoque de mejora continua mediante la evaluación post-incidente, la integración de lecciones aprendidas y el fortalecimiento progresivo de la madurez de ciberseguridad de TechCo.



3. Marco de Referencia: NIST Cybersecurity Framework

El **NIST Cybersecurity Framework (CSF)** proporciona a TechCo una estructura estratégica para gestionar el riesgo cibernético de manera coherente con los objetivos del negocio. A continuación, se desarrollan las cinco funciones del framework, enfocadas específicamente al escenario de ransomware, destacando el **resultado estratégico esperado** en cada una.

3.1 Identificar (Identify)

Objetivo estratégico: Comprender el contexto del negocio, los activos críticos y los riesgos de ransomware para priorizar adecuadamente las inversiones y decisiones de seguridad. Resultados esperados: - Visibilidad completa de los activos críticos de información, sistemas y procesos que soportan los servicios de TechCo. - Identificación clara de dependencias tecnológicas y de negocio, incluyendo terceros y servicios cloud. - Evaluación formal del riesgo de ransomware basada en impacto operativo, financiero, legal y reputacional. - Priorización de riesgos que permita enfocar recursos en los activos con mayor impacto para el negocio.

3.2 Proteger (Protect)

Objetivo estratégico: Reducir de forma significativa la probabilidad de éxito de un ataque de ransomware mediante controles preventivos alineados al riesgo.
Resultados esperados: - Implementación de controles de seguridad consistentes y estandarizados en toda la organización. - Reducción del riesgo de propagación lateral gracias a segmentación de red y principios Zero Trust. - Protección efectiva de endpoints, identidades y credenciales frente a malware y accesos no autorizados. - Resiliencia operativa reforzada mediante estrategias de backup seguras, aisladas e inmutables.

3.3 Detectar (Detect)

Objetivo estratégico: Identificar de manera temprana actividades maliciosas asociadas a ransomware para limitar su impacto antes de que se materialice a gran escala.
Resultados esperados: - Capacidad de monitoreo continuo de eventos de seguridad relevantes en tiempo casi real. - Detección temprana de comportamientos anómalos en usuarios, sistemas y red. - Disminución del tiempo medio de detección (MTTD) de incidentes de ransomware. - Activación oportuna de alertas que permitan una respuesta rápida y coordinada.

3.4 Responder (Respond)

Objetivo estratégico: Contener y gestionar eficazmente un incidente de ransomware minimizando el daño al negocio y asegurando una toma de decisiones informada.
Resultados esperados: - Activación inmediata y coordinada del plan de respuesta a incidentes. - Contención rápida del ransomware para evitar su propagación a otros sistemas críticos. - Gestión estructurada de la comunicación interna, externa y regulatoria. - Reducción del impacto financiero, operativo y reputacional del incidente.

3.5 Recuperar (Recover)

Objetivo estratégico: Restaurar los servicios críticos de TechCo de manera segura y priorizada, fortaleciendo la resiliencia futura de la organización.
Resultados esperados: - Recuperación controlada de sistemas y datos desde respaldos confiables y verificados. - Restablecimiento oportuno de los servicios críticos conforme a los objetivos de continuidad del negocio. - Validación de la integridad y seguridad de los sistemas antes de su retorno a producción. - Incorporación de lecciones aprendidas para mejorar la postura de ciberseguridad y la resiliencia organizacional.

4. Identificación (Identify)

La función **Identificar** del NIST CSF establece las bases para una gestión eficaz del riesgo de ransomware, permitiendo a TechCo comprender qué debe proteger, por qué es crítico para el negocio y cuáles son las consecuencias de un compromiso de seguridad.
Desde una perspectiva estratégica, esta función habilita una toma de decisiones informada por parte de la alta dirección, alineando la ciberseguridad con los objetivos corporativos y la continuidad del negocio.

4.1 Activos Críticos Afectados

Desde una perspectiva ejecutiva, la identificación de los activos críticos afectados por el incidente de ransomware es fundamental para comprender el impacto real sobre el negocio de TechCo. Estos activos no solo representan componentes tecnológicos, sino habilitadores directos de la continuidad operativa, el cumplimiento regulatorio y la confianza de los clientes. La indisponibilidad o el compromiso de cualquiera de estos activos tiene consecuencias inmediatas en los ingresos, la reputación corporativa y la sostenibilidad de la organización.
Los activos críticos identificados en el incidente incluyen:

- **Servidor de archivos corporativo**
  - Soporta la operación diaria y la colaboración interna.
  - Su indisponibilidad genera interrupciones inmediatas en los procesos de negocio.
- **Base de datos de clientes**
  - Contiene información personal y financiera sensible.
  - Constituye un activo de alto valor desde la perspectiva regulatoria y reputacional.
- **Sistemas de backup internos**
  - Diseñados para garantizar la recuperación ante desastres.
  - Su compromiso evidencia una arquitectura de respaldo inadecuada.
- **Infraestructura de red interna**
  - Elemento habilitador de la propagación lateral del ransomware.
  - Falta de controles de segmentación y monitoreo.

4.2 Vulnerabilidades Identificadas

El análisis del incidente permitió identificar vulnerabilidades estructurales y operativas:

- Bajo nivel de concientización del personal frente a ataques de phishing.
- Arquitectura de red plana sin segmentación lógica.
- Backups conectados permanentemente a la red productiva.
- Ausencia de monitoreo continuo y alertas tempranas.
- Gestión insuficiente de identidades, accesos y privilegios.

4.3 Evaluación de Riesgos

Desde una perspectiva ejecutiva, la evaluación de riesgos permite a la alta dirección de TechCo comprender de manera estructurada cómo las amenazas de ransomware se materializan en impactos concretos para el negocio. Esta evaluación considera tanto la **probabilidad de ocurrencia** como el **impacto potencial**, facilitando la priorización de decisiones y la asignación eficiente de recursos.
A continuación, se presenta la matriz de evaluación de riesgos asociada al incidente de ransomware:

ID Riesgo	Descripción del Riesgo	Impacto	Probabilidad	Riesgo Identificado	Posibles Soluciones / Tratamiento
R-01	Infección inicial por phishing que permite la ejecución de ransomware en estaciones de trabajo	Alto	Alto	Compromiso de credenciales y punto de entrada inicial del ataque	Programas de concientización, filtrado avanzado de correo, sandboxing y MFA
R-02	Propagación lateral del ransomware a servidores críticos	Muy Alto	Alto	Arquitectura de red plana sin segmentación	Segmentación de red, Zero Trust, control de tráfico lateral
R-03	Cifrado de la base de datos de clientes	Muy Alto	Medio	Exposición de datos sensibles y riesgo regulatorio	Cifrado de datos, control de accesos, monitoreo y clasificación de información
R-04	Compromiso de sistemas de backup internos	Alto	Alto	Backups no aislados ni inmutables	Backups air-gapped, backups inmutables y pruebas periódicas de restauración
R-05	Detección tardía del incidente de ransomware	Alto	Alto	Ausencia de monitoreo continuo y alertas tempranas	Implementación de SIEM, EDR/XDR y protocolos de alerta
R-06	Interrupción prolongada de servicios cloud ofrecidos a clientes	Muy Alto	Medio	Dependencia directa de sistemas afectados	Planes de continuidad, entornos altemos y DRP
R-07	Daño reputacional y pérdida de confianza de clientes	Muy Alto	Medio	Comunicación reactiva y falta de preparación	Plan de comunicación de crisis y gestión de stakeholders

La materialización de estos riesgos evidenció una postura de seguridad reactiva. Su tratamiento efectivo permitirá a TechCo reducir significativamente su exposición futura al ransomware y fortalecer su resiliencia organizacional.

4.4 Resultado Estratégico de la Función Identificar

Como resultado de una correcta implementación de esta función, TechCo debe alcanzar:

- Visibilidad integral de sus activos críticos y dependencias de negocio.
- Priorización de riesgos basada en impacto y probabilidad.
- Alineación de las inversiones en ciberseguridad con los objetivos estratégicos.
- Base sólida para la implementación efectiva de las funciones Proteger, Detectar, Responder y Recuperar.

4.5 Tabla Resumen – NIST CSF aplicado a TechCo

Función NIST CSF	Enfoque Estratégico	Resultado para TechCo
Identificar	Comprensión del contexto, activos y riesgos	Priorización clara de activos críticos y riesgos de ransomware
Proteger	Controles preventivos alineados al riesgo	Reducción de la probabilidad de infección y propagación
Detectar	Monitoreo y alerta temprana	Disminución del tiempo de detección del ransomware
Responder	Gestión coordinada del incidente	Contención rápida y reducción del impacto al negocio
Recuperar	Restauración y resiliencia	Continuidad operativa y fortalecimiento post-incidente

5. Protección (Protect)

5.1 Controles Preventivos Clave

Desde una perspectiva ejecutiva, los controles preventivos constituyen la **primera y más costo-efectiva línea de defensa** frente a ataques de ransomware. Su objetivo no es únicamente reducir la superficie de ataque, sino **interrumpir la cadena de ataque en sus fases iniciales**, evitando que una amenaza técnica se convierta en una crisis de negocio.

La implementación de controles preventivos debe responder a un enfoque **basado en riesgos**, priorizando aquellos controles que protegen los activos más críticos y que reducen de manera tangible la probabilidad de infección, propagación y cifrado masivo de información. Estos controles deben estar respaldados por políticas formales, patrocinio de la alta dirección y una ejecución consistente en toda la organización.

Los controles preventivos descritos a continuación representan **capacidades estratégicas**, no solo soluciones técnicas aisladas, y deben integrarse como parte del modelo de gobierno y gestión de la ciberseguridad de TechCo.

5.1.1 Seguridad del correo electrónico

Desde una perspectiva ejecutiva, el correo electrónico representa el **principal vector de entrada de ataques de ransomware** y, por tanto, uno de los riesgos más relevantes para TechCo. La seguridad del correo no debe abordarse únicamente como un control técnico, sino como una capacidad estratégica de protección del negocio.

Para TechCo, fortalecer la seguridad del correo electrónico tiene como resultado directo la reducción significativa del riesgo de infección inicial y la protección de los usuarios frente a técnicas de ingeniería social cada vez más sofisticadas.

Medidas estratégicas clave:

- Implementación de filtros avanzados anti-phishing con análisis de reputación, contenido y comportamiento.
- Uso de sandboxing para el análisis dinámico de archivos adjuntos y enlaces.
- Bloqueo sistemático de adjuntos ejecutables, macros y formatos de alto riesgo.
- ntegración de campañas periódicas de simulación de phishing como mecanismo de control preventivo.

Resultado estratégico: Disminución del riesgo de compromiso inicial y fortalecimiento de la primera línea de defensa humana y tecnológica.

5.1.2 Segmentación de red

La ausencia de segmentación de red fue uno de los factores determinantes en la rápida propagación del ransomware dentro de TechCo. Desde un enfoque ejecutivo, la segmentación constituye un **control crítico para limitar el impacto** de un incidente una vez que el atacante ha logrado acceso inicial.
La segmentación debe diseñarse en función del riesgo y del valor de los activos, separando entornos de usuarios, servidores críticos, backups y servicios expuestos.
Medidas estratégicas clave: - Separación lógica y física de entornos productivos, de respaldo y de usuarios finales. - Implementación de microsegmentación y controles de acceso basados en identidad. - Aplicación de principios Zero Trust para el tráfico interno.

- **Resultado estratégico:** Contención efectiva del ransomware y reducción drástica del impacto operacional.

5.1.3 Gestión de accesos

La gestión inadecuada de identidades y privilegios incrementa exponencialmente el impacto de un ataque de ransomware. Desde la alta dirección, este dominio debe entenderse como un **factor habilitador de control y gobernanza**, no solo como una función técnica.

Medidas estratégicas clave: - Aplicación estricta del principio de mínimo privilegio. - Uso obligatorio de autenticación multifactor (MFA) para accesos críticos y remotos. - Revisión periódica y formal de cuentas privilegiadas.

- **Resultado estratégico:** Reducción del riesgo de escalamiento de privilegios y compromiso de sistemas críticos.

5.1.4 Protección de endpoints

Los endpoints representan el punto donde convergen usuarios, datos y procesos de negocio. Una protección avanzada de endpoints es esencial para detectar y contener ransomware antes de que se propague.
Medidas estratégicas clave: - Implementación de soluciones EDR/XDR con capacidades de detección basada en comportamiento. - Contención automática y aislamiento de equipos comprometidos. - Hardening de sistemas y gestión rigurosa de parches.

- **Resultado estratégico:** Reducción del tiempo de exposición y contención temprana del ataque.

5.1.5 Estrategia de backups

La estrategia de respaldos es un pilar fundamental de la resiliencia frente a ransomware. Desde una visión ejecutiva, los backups representan la **capacidad real de recuperación del negocio**. Medidas estratégicas clave: - Implementación de backups fuera de línea (air-gapped). - Uso de backups inmutables protegidos contra borrado o cifrado. - Pruebas periódicas de restauración y validación.

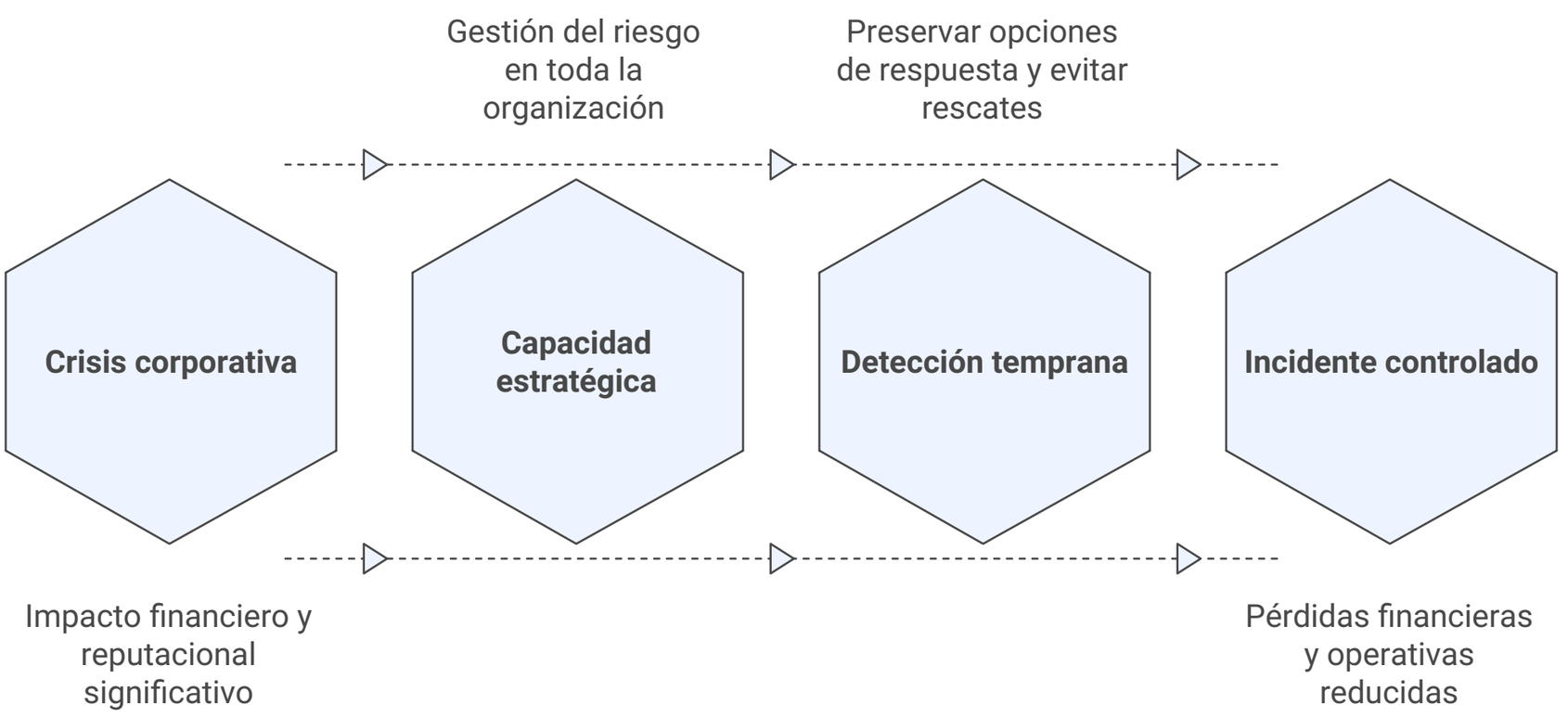
Resultado estratégico: Capacidad de recuperación confiable sin dependencia del pago de rescates.

6. Detección (Detect)

Desde una perspectiva ejecutiva, la función de **Detección** es uno de los principales diferenciadores entre un incidente controlado y una crisis corporativa de gran impacto. En el contexto del ransomware, la capacidad de detectar actividades maliciosas en sus fases iniciales tiene un efecto directo en la reducción de pérdidas financieras, interrupciones operativas, exposición regulatoria y daño reputacional.

Para TechCo, la detección no debe concebirse únicamente como una función técnica del área de TI, sino como una **capacidad estratégica de gestión del riesgo**, estrechamente vinculada a la continuidad del negocio y a la resiliencia organizacional. Una detección temprana permite a la organización ganar tiempo, preservar opciones de respuesta y evitar decisiones forzadas como el pago de rescates.

Detección temprana de ransomware para la resiliencia empresarial



6.1 Capacidades de Detección Temprana

TechCo debe consolidar una capacidad robusta de detección temprana basada en el monitoreo continuo, la correlación de eventos y el análisis de comportamientos anómalos en todo su ecosistema tecnológico.

Desde el punto de vista ejecutivo, estas capacidades permiten: - Obtener visibilidad centralizada del estado de seguridad de la organización. - Identificar patrones de ataque antes de que se produzca el cifrado masivo de información. - Reducir de forma significativa el **Tiempo Medio de Detección (MTTD)**.

Capacidades estratégicas recomendadas: - Implementación de una plataforma **SIEM** para la correlación de eventos de seguridad provenientes de múltiples fuentes. - Uso de soluciones **EDR/XDR** con detección basada en comportamiento y análisis de amenazas. - Monitoreo del tráfico de red, especialmente de movimientos laterales y accesos a sistemas críticos. - Integración de inteligencia de amenazas (Threat Intelligence) relevante para ransomware.

- **Resultado estratégico:** Capacidad de identificar incidentes de ransomware en etapas tempranas, reduciendo de manera sustancial su alcance e impacto.

6.2 Protocolo de Alerta Temprana

Un protocolo de alerta temprana es el mecanismo que transforma la detección técnica en **acción organizacional inmediata**. Sin un proceso claro de escalamiento y toma de decisiones, incluso las mejores herramientas de detección pierden efectividad.
Desde una visión ejecutiva, este protocolo debe garantizar que los eventos críticos sean reconocidos, evaluados y atendidos con la urgencia adecuada, evitando retrasos que amplifiquen el impacto del incidente.

Elementos clave del protocolo: - Definición clara de eventos y umbrales que requieren escalamiento inmediato. - Notificación automática al Equipo de Respuesta a Incidentes (CSIRT). - Procedimientos de escalamiento hacia la alta dirección y el CISO según la severidad. - Registro y trazabilidad de alertas para fines de auditoría y mejora continua.

- **Resultado estratégico:** Activación oportuna del plan de respuesta, coordinación efectiva entre equipos y minimización del impacto operativo y financiero del incidente.

6.3 Indicadores Clave de Desempeño en Detección

Para asegurar la efectividad de la función Detectar, TechCo debe definir y monitorear indicadores clave que permitan a la alta dirección evaluar el desempeño de esta capacidad. Indicadores estratégicos recomendados: - Tiempo Medio de Detección (MTTD). - Porcentaje de incidentes detectados de forma proactiva. - Número de alertas críticas correctamente escaladas. - Reducción del alcance del incidente al momento de la detección.

- **Resultado estratégico:** Gobierno efectivo de la función de detección y toma de decisiones basada en métricas objetivas.

7. Respuesta (Respond)

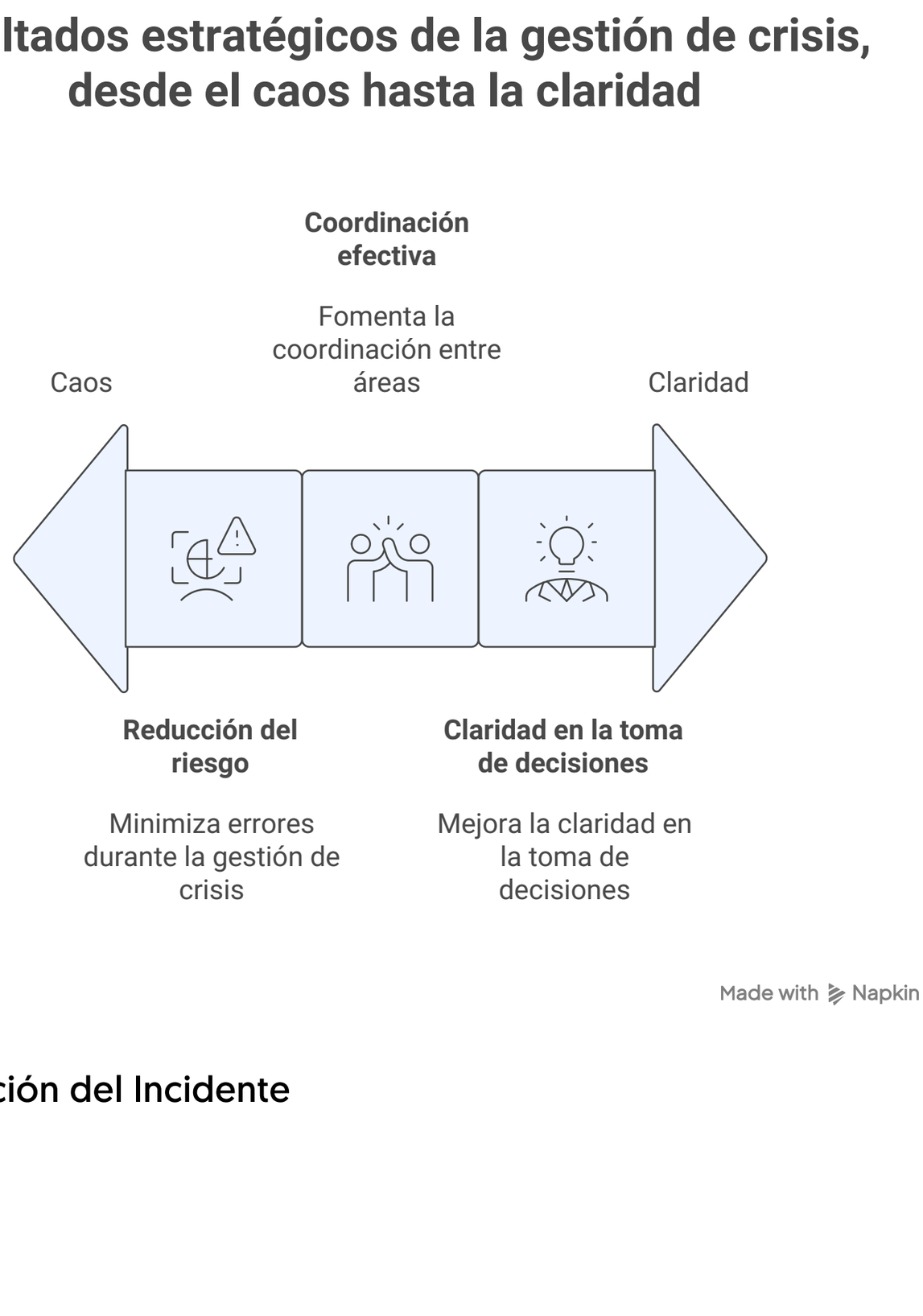
La función **Responder** representa la capacidad de TechCo para gestionar de manera efectiva un incidente de ransomware una vez que ha sido detectado. Desde una perspectiva ejecutiva, esta función es crítica para **contener la crisis, preservar la continuidad del negocio, proteger a los clientes y salvaguardar la reputación corporativa**.

Una respuesta eficaz no depende únicamente de capacidades técnicas, sino de una **gobernanza clara, liderazgo definido y toma de decisiones oportuna**, alineadas con el apetito de riesgo y los objetivos estratégicos de la organización.

7.1 Activación del Plan de Respuesta

La activación temprana y estructurada del Plan de Respuesta a Incidentes es fundamental para evitar que un ataque de ransomware escale de un evento técnico a una crisis corporativa. Desde el punto de vista de la alta dirección, este proceso debe garantizar rapidez, claridad y control.

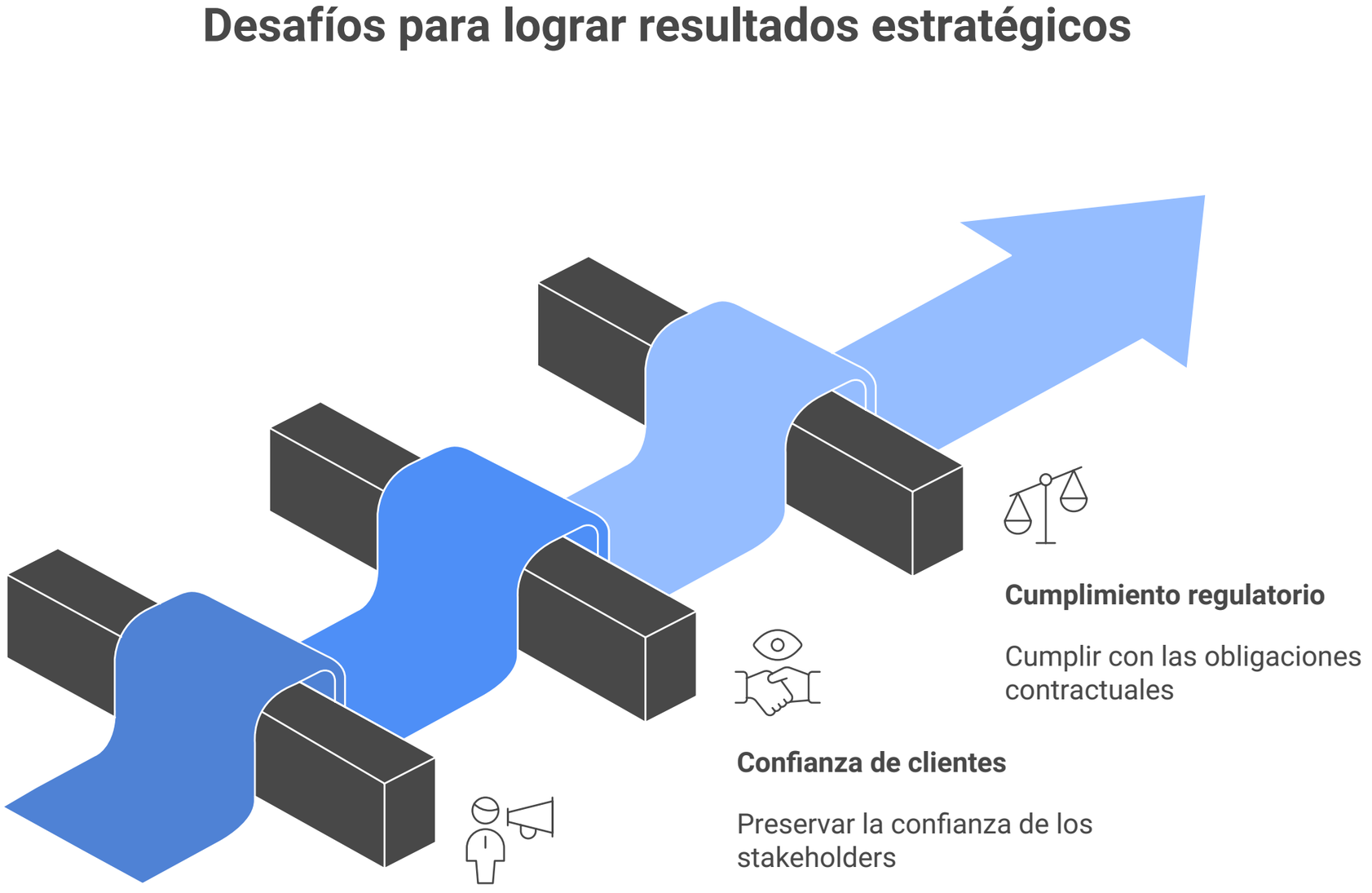
Elementos clave de la activación: - Confirmación del incidente y su clasificación según nivel de severidad. - Activación inmediata del Equipo de Respuesta a Incidentes (CSIRT). - Aislamiento de los sistemas afectados para contener la propagación. - Preservación de evidencias para análisis forense y posibles acciones legales.



7.3 Comunicación del Incidente

La comunicación durante un incidente de ransomware es un factor determinante en la protección de la reputación y la confianza de clientes, socios y reguladores. Desde un enfoque ejecutivo, la comunicación debe ser **controlada, coherente y alineada con la estrategia corporativa**.

Principios estratégicos de comunicación: - Comunicación interna temprana y clara para evitar rumores y desinformación. - Notificación externa a clientes y terceros cuando sea requerido, de forma transparente y responsable. - Cumplimiento de plazos regulatorios de notificación de incidentes. - Coordinación del mensaje con el área legal para mitigar riesgos legales y reputacionales.



8. Recuperación (Recover)

La recuperación efectiva es un habilitador directo de la resiliencia organizacional y de la confianza de clientes y stakeholders.

8.1 Restauración de Sistemas

Resultados estratégicos: - Retorno seguro y controlado a la operación normal. - Protección de la integridad de la información.

8.2 Continuidad del Negocio

Resultados estratégicos: - Cumplimiento de objetivos de continuidad. - Reducción del impacto financiero prolongado.

9. Mejora Continua

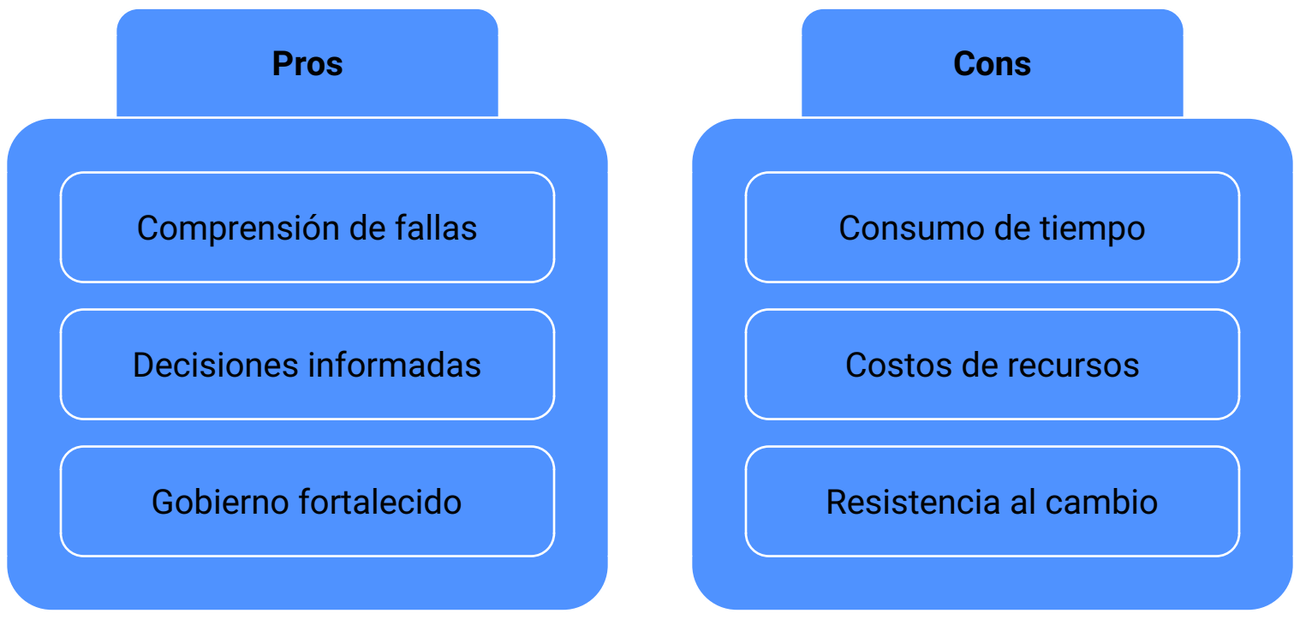
La **Mejora Continua** es un componente esencial del modelo de resiliencia cibernética de TechCo y un habilitador clave para la sostenibilidad del negocio en el largo plazo. Desde una perspectiva ejecutiva, esta función garantiza que cada incidente de ransomware — independientemente de su severidad— se traduzca en un fortalecimiento tangible de la postura de seguridad, y no en una repetición de fallas pasadas.

La mejora continua permite a la alta dirección evaluar objetivamente la eficacia del plan de respuesta, optimizar la asignación de recursos y elevar progresivamente el nivel de madurez de ciberseguridad de la organización, alineándolo con el apetito de riesgo y los objetivos estratégicos de TechCo.

9.1 Evaluación Post-Incidente

La evaluación post-incidente constituye un proceso formal y estructurado mediante el cual TechCo analiza de manera integral la gestión del incidente de ransomware. Este ejercicio debe realizarse una vez estabilizada la operación, involucrando a las áreas técnicas, de negocio, legales y de dirección.

Desde un enfoque ejecutivo, esta evaluación tiene como propósito principal proporcionar **visibilidad clara y objetiva** sobre el desempeño organizacional durante el incidente. Aspectos clave de la evaluación: - Análisis de causa raíz (Root Cause Analysis) del incidente. - Evaluación de la efectividad de los controles preventivos, de detección y de respuesta. - Medición del impacto real en términos operativos, financieros, legales y reputacionales. - Revisión del cumplimiento de tiempos de detección, contención y recuperación.



9.2 Lecciones Aprendidas

La consolidación de lecciones aprendidas transforma la experiencia del incidente en conocimiento organizacional. Desde la alta dirección, este proceso asegura que los errores no se repitan y que las buenas prácticas se institucionalicen.

Las lecciones aprendidas deben documentarse formalmente y traducirse en acciones concretas, evitando que queden como ejercicios teóricos sin impacto real.

9.3 Madurez en Ciberseguridad

El fortalecimiento de la madurez en ciberseguridad debe ser un objetivo estratégico permanente para TechCo. Desde una visión ejecutiva, la madurez refleja la capacidad de la organización para anticipar, resistir, responder y recuperarse de amenazas cibernéticas de manera sistemática y predecible. TechCo debe evaluar periódicamente su nivel de madurez utilizando marcos reconocidos como el NIST CSF, identificando brechas y estableciendo hojas de ruta de mejora progresiva.

10. Conclusión Ejecutiva

El incidente de ransomware sufrido por TechCo confirma que las amenazas cibernéticas ya no constituyen un riesgo exclusivamente tecnológico, sino un **riesgo estratégico de negocio** con impacto directo en la continuidad operativa, la confianza de los clientes, el cumplimiento regulatorio y la sostenibilidad financiera de la organización.

Este Plan de Respuesta a Incidentes, alineado al **NIST Cybersecurity Framework (CSF)**, proporciona a TechCo un marco estructurado para anticipar, resistir, responder y recuperarse de ataques de ransomware de manera coherente con sus objetivos corporativos. Su adopción permite a la organización evolucionar desde una postura reactiva hacia un modelo de **resiliencia cibernética**, donde la seguridad de la información se integra como un habilitador del negocio y no como un obstáculo operativo.

Finalmente, la eficacia de este plan dependerá del **compromiso sostenido de la alta dirección**, de su integración con la gestión de riesgos empresariales y de un enfoque de mejora continua. En un entorno de amenazas dinámico, la resiliencia cibernética se consolida como una ventaja competitiva clave para TechCo y como un factor crítico para su crecimiento y permanencia en el mercado.

11. Revisión por la Dirección

La **Revisión por la Dirección** constituye un componente esencial del gobierno de la ciberseguridad y un requisito clave para asegurar la vigencia, eficacia y alineación estratégica del Plan de Respuesta a Incidentes de Ransomware de TechCo. Desde una perspectiva ejecutiva, esta revisión permite a la alta dirección ejercer una supervisión activa sobre la gestión del riesgo cibernético y garantizar que la ciberseguridad se integre plenamente en la toma de decisiones corporativas.

11.1 Objetivo de la Revisión

El objetivo principal de la revisión por la dirección es evaluar de manera periódica si el plan de respuesta:

- Continúa siendo adecuado frente al panorama actual de amenazas.
- Es eficaz para proteger los objetivos estratégicos y la continuidad del negocio.
- Se encuentra alineado con el apetito de riesgo definido por la organización.

11.2 Alcance de la Revisión Ejecutiva

La revisión debe realizarse al menos de forma anual, y adicionalmente después de incidentes relevantes de ciberseguridad o cambios significativos en el negocio o el entorno regulatorio. Los aspectos a revisar incluyen:

- Resultados de incidentes de ransomware y evaluaciones post-incidente.
- Nivel de cumplimiento del Plan de Respuesta a Incidentes.
- ndicadores clave de desempeño y riesgo (KPIs/KRIs).
- Estado de implementación de las acciones de mejora continua.
- Cambios en riesgos, amenazas, tecnologías y dependencias críticas.

11.3 Resultados Esperados de la Revisión

Como resultado de una revisión efectiva por la dirección, TechCo debe lograr:

- Validación ejecutiva de la eficacia del plan de respuesta.
- Priorización de inversiones en ciberseguridad basada en riesgos reales.
- Ajustes estratégicos al plan, políticas y controles de seguridad.
- Refuerzo del compromiso organizacional con la resiliencia cibernética.

Proceso de Revisión de la Dirección para el Plan de Respuesta a Ransomware