Grant Thornton

Cámara MADRID

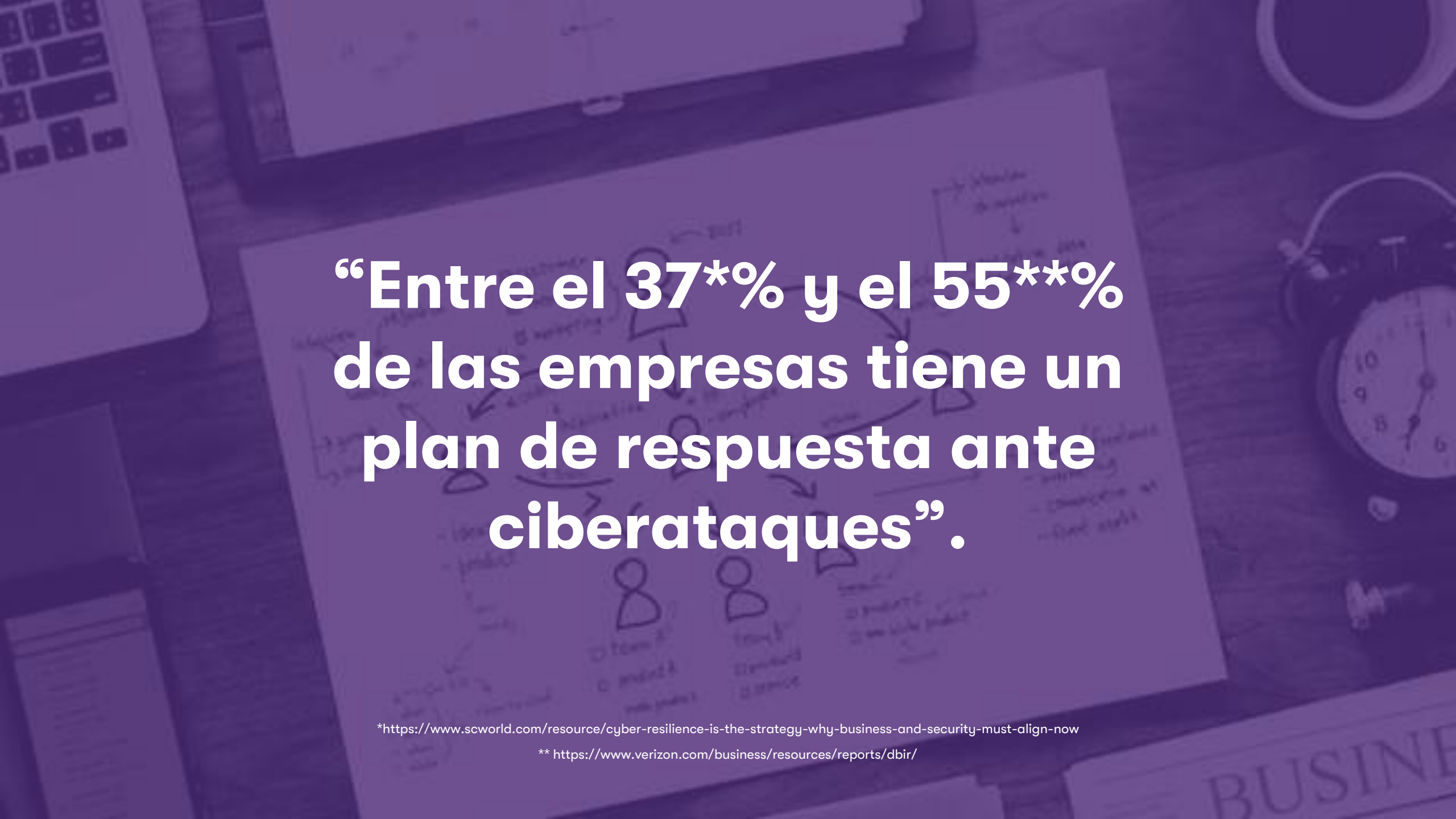
Primeras horas tras un ciberataque: respuestas rápidas y efectivas sin comprometer el negocio

11 de marzo

Cristina Muñoz-Aycuens

Socia de Forensic y Ciberseguridad de Grant Thornton

Índice



“Entre el 37*% y el 55**% de las empresas tiene un plan de respuesta ante ciberataques”.

*https://www.scworld.com/resource/cyber-resilience-is-the-strategy-why-business-and-security-must-align-now

** https://www.verizon.com/business/resources/reports/dbir/


“El 42% de las empresas que tienen un plan de respuesta no lo actualiza de forma periódica”.
https://www.ponemon.org/

“Sólo el 30% de las empresas prueba sus planes de respuesta”.

https://www.cisa.gov/

Ciberataques

Algunos números

- El **tiempo promedio** para detectar una brecha es **de 204 días**, lo que equivale a casi siete meses antes de que las empresas se den cuenta de que han sido comprometidas.
- Se necesitan otros **54 días,** en promedio, **para contener una brecha**, lo que significa que la mayoría de las empresas tardan más de ocho meses en gestionar completamente un incidente.
- Las empresas que utilizan **seguridad basada en IA** reducen su tiempo de detección de brechas a la mitad, lo que finalmente lo **reduce** a un promedio de **102 días**.
- Los **ataques de ransomware** se intensifican rápidamente: las organizaciones tienen un promedio de **solo cuatro horas** para responder antes de que el daño sea irreversible.
- Las empresas con **sistemas de detección automatizados** contienen las amenazas **un 40 % más rápido**.

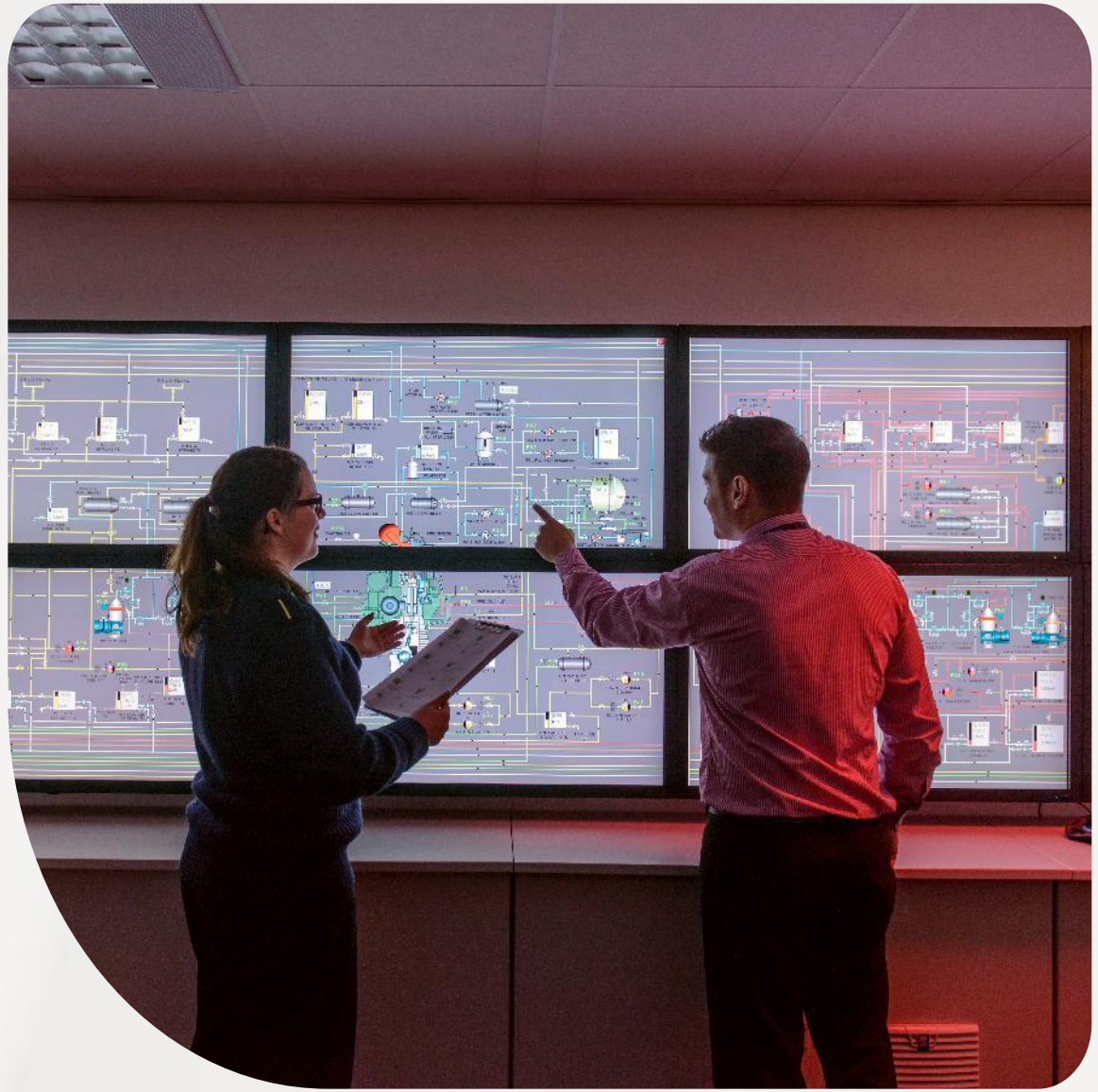
Grant Thornton

Cámara MADRID

Ciberataques

Algunos números

- El **68%** de las brechas de seguridad **implican un factor humano**, ya sea mediante phishing, contraseñas débiles o configuraciones incorrectas.
- **Solo** el **45% de los empleados recibe capacitación** en ciberseguridad, lo que deja a más de la mitad de la fuerza laboral sin preparación para ataques de phishing e ingeniería social.
- Las organizaciones que **capacitan** a sus empleados **trimestralmente reducen** los incidentes de seguridad **en un 60%,** en comparación con aquellas que ofrecen capacitación una vez al año (o no la ofrecen).
- El **40% de las empresas no revoca el acceso de ex empleados a sistemas críticos**, lo que los expone a amenazas internas.
- Las **configuraciones incorrectas** de la **nube** son responsables del **19% de las brechas de seguridad**, a menudo causadas por errores humanos en la gestión de TI.



Las primeras 24-72 horas tras un ciberataque

Grant Thornton

Cámara MADRID

Primeras 24-72h

Qué suele desencadenar el incidente

- Phishing o ingeniería social muy convincente.
- Vulnerabilidad conocida, pero sin parchear.
- Compromiso de un proveedor (muy común).
- Robo de credenciales (MFA bypass / token theft).
- Exposición accidental de activos en internet.

Grant Thornton Cámara MADRID

Primeras 24-72h

La cronología típica de un ataque

Minutos 0-60

Detección parcial, alertas difusas.

Hora 1-3

Progresión del atacante → movimiento lateral, AD reconnaissance.

Hora 3-6

Detonación (cifrado / destrucción / exfiltración).

Hora 6-12

Caos operativo → caída de servicios, pánico técnico.

Primeras 24h

Necesidad de decisiones estratégicas.

Primeras 72h

Estabilización, análisis de daños, primeras comunicaciones regulatorias.

Grant Thornton

Cámara MADRID

Primeras 24-72h

Decisiones críticas de las primeras horas

Aislar o apagar

- Apagar toda la red: máxima protección, pero riesgo de paralizar el negocio.
- Aislar zonas: requiere madurez técnica y rapidez.

¿Restaurar o preservar evidencias?

- Restaurar muy pronto puede destruir evidencia clave.
- Preservar puede retrasar el retorno a la normalidad.

Uso de canales alternativos de comunicación

- Teams/correo pueden estar monitorizados o comprometidos.
- Pasar a teléfonos personales o canales predefinidos.

Activación del Comité de Crisis

- TI / Ciberseguridad
- Legal
- Comunicación
- Negocio
- CEO / Dirección
- Compliance & DPO si hay datos personales

Primeras 24-72h

Errores más frecuentes en las primeras 72 horas

- Reiniciar servidores afectados (el peor error)
- Comunicar a destiempo a prensa o empleados
- Restaurar backups sin verificarlos
- Caos en roles y responsabilidades
- Minimizar el incidente (“parece que ya va funcionando todo”)
- No notificar a proveedores críticos

Grant Thornton | Cámara MADRID

Primeras 24-72h

Qué sí funciona

- Protocolos y roles claros.
- Procedimientos ensayados.
- Equipo reducido para decisiones clave.
- Comunicación simple, directa y repetida.

Impacto regulatorio: NIS2 y DORA en la respuesta a incidentes

Grant Thornton

Cámara MADRID

Impacto regulatorio

Por qué ahora es más crítico responder bien

La regulación ya no se limita a pedir controles; ahora exige:

- Rapidez
- Transparencia
- Coordinación interdepartamental
- Evidencias formales

Ya en el 2022… la UE empezó a combatir las amenazas cibernéticas

La UE lleva trabajando en varias líneas de trabajo desde hace varios años para:

1. Promover la ciberresiliencia.
2. Luchar contra la ciberdelincuencia.
3. Impulsar la ciberdiplomacia y la ciberdefensa.

Se establecen nuevos requisitos de seguridad como la **respuesta ante incidentes**, la seguridad en la cadena de suministro, el cifrado y la divulgación de vulnerabilidades.

Las empresas deben tener un **plan de respuesta ante incidentes** que incluya una descripción detallada de lo que constituye un ciberataque, cómo deben responder los empleados y cómo se restablecerán las operaciones en caso de que se produzca una infracción.

Las empresas deben **notificar los incidentes** cuando se produzcan para que los reguladores puedan evaluar sus vulnerabilidades y hacer recomendaciones para mejorar su postura de seguridad.

Grant Thornton Cámara MADRID

Impacto regulatorio

NIS2 - Qué exige realmente

Notificación en tres fases

- *Early Warning:* 24 horas.
- *Informe de seguimiento:* 72 horas.
- *Informe final:* 1 mes.

Capacidades obligatorias
(no "recomendadas")

- Detección avanzada.
- Gestión de vulnerabilidades.
- Respuesta a incidentes.
- Continuidad operativa y recuperabilidad.

Gobernanza reforzada

- El órgano de administración es responsable.
- Debe aprobar políticas, supervisar riesgos y asegurarse de que existe capacidad de respuesta.

Sanciones importantes

- Económicas, pero también reputacionales.
- Posibles responsabilidades personales.

Impacto regulatorio

DORA — En entidades financieras y tecnológicas críticas

Gestión integral del riesgo TIC

- No se trata solo de ciberseguridad: continuidad, proveedores, datos, integridad operativa.

Supervisión de terceros esenciales

- Cloud, core bancario, procesadores, etc.
- Contratos reforzados, reportabilidad, trazabilidad.

Testing obligatorio

- Simulacros anuales.
- Pruebas avanzadas (incluido threat-led testing) para entidades críticas.

Obligación de reportar incidentes severos

- Tiempos estrictos.
- Formato estandarizado.
- Impacto en clientes y operaciones.

Impacto regulatorio

Cómo afecta a la práctica real

No basta con “responder”: hay que generar evidencia.

Afecta al timing interno: la notificación se solapa con la fase de contención.

Obliga a tener un **mapa de proveedores** perfectamente actualizado.

Eleva la importancia de legal & compliance dentro del comité de crisis.

Grant Thornton

Cámara MADRID

Lecciones aprendidas de crisis reales

Grant Thornton

Cámara MADRID

Lecciones aprendidas de Crisis Reales

Lección 1: La improvisación es el enemigo número uno

- Empresas sin procedimientos acaban tomando decisiones contradictorias.
- El coste de improvisar suele multiplicar por 3–4 el tiempo de recuperación.

Lección 2: Las crisis no se ganan con más gente, sino con roles claros

- Equipos de 20 personas en un call → improductivo.
- Equipo núcleo de 6–8 personas → óptimo.

Lecciones aprendidas de Crisis Reales

Lección 3: Backups no significan recuperabilidad

- Copias cifradas o manipuladas.
- Tiempos de restauración de días o semanas.
- Backups sin pruebas de integridad.

Lección 4: Los proveedores son una extensión del riesgo

- SLA irreales.
- Dependencias ocultas.
- Exposición a terceros no evaluada.

Lecciones aprendidas de Crisis Reales

Lección 5: La comunicación es el principal vector de daño reputacional

- Mensajes improvisados → titulares negativos.
- Empleados difundiendo información por WhatsApp.
- Clientes informándose por prensa antes que por la empresa.

Lección 6: Las organizaciones entrenadas sufren menos

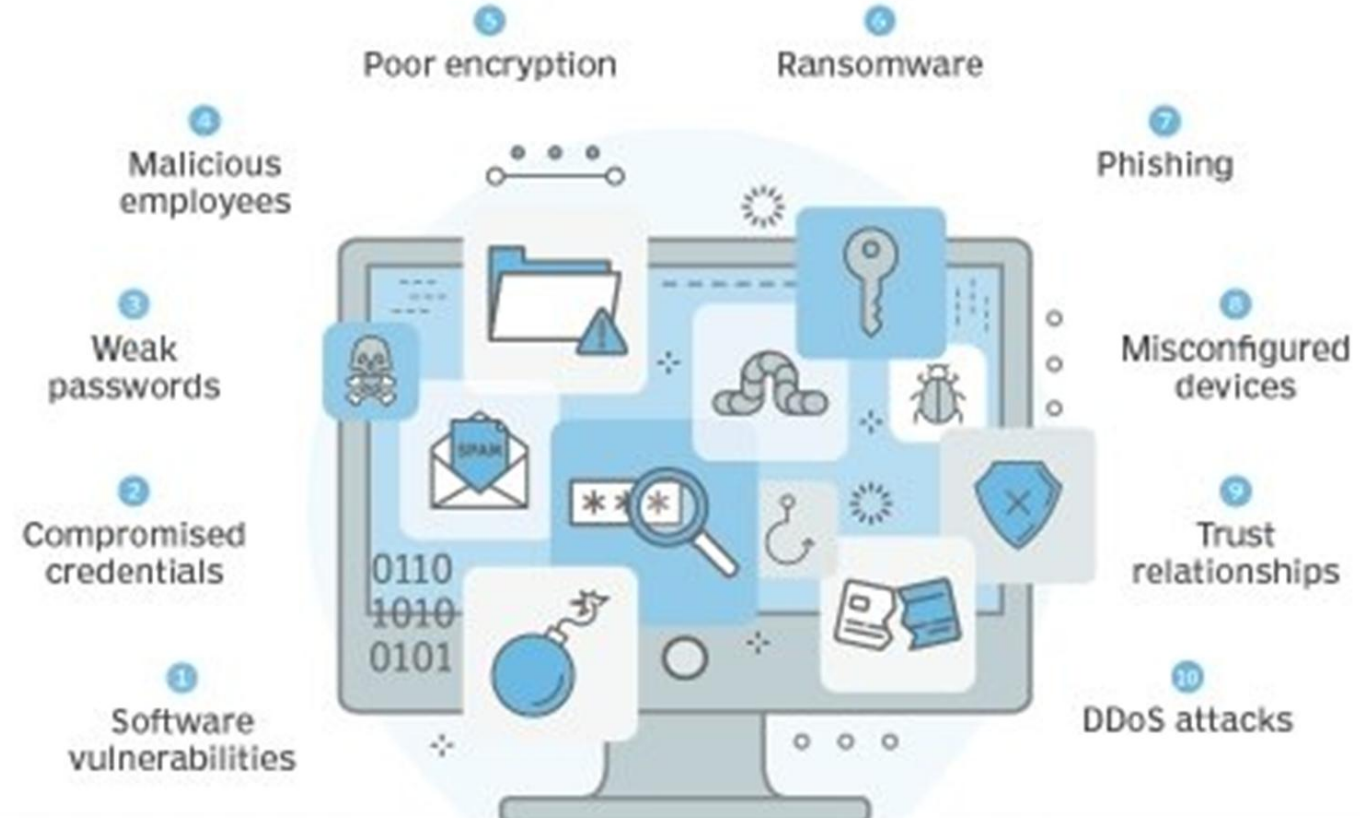
- Simulacros reales cambian la velocidad y la coordinación.
- Las empresas que ensayan reaccionan en minutos, no en horas.

Caso práctico: “Te acaban de cifrar los sistemas, ¿qué haces ahora?”

Grant Thornton

Cámara MADRID

10 common attack vectors



09:07 de la mañana

La gente empieza a avisar:

- “No puedo entrar al correo.”
- “El sistema va lentísimo…”
- “Todos mis archivos se han convertido en un nombre raro.”

De repente aparece un mensaje:
“Tus datos han sido cifrados. Para recuperarlos, paga.”

¿Qué decides?

OPCIÓN A

“Reiniciamos los ordenadores, a ver si se arregla”

OPCIÓN B

“Paramos y avisamos: esto es un incidente serio”

09:07 de la mañana

La gente empieza a avisar:

- “No puedo entrar al correo.”
- “El sistema va lentísimo…”
- “Todos mis archivos se han convertido en un nombre raro.”

De repente aparece un mensaje:
“Tus datos han sido cifrados. Para recuperarlos, paga.”

¿Qué decides?

OPCIÓN A

“Reiniciamos los ordenadores, a ver si se arregla”

Peor decisión posible. Un reinicio puede activar más cargas del atacante y extender el daño. Pierdes evidencia, aceleras el ataque y todo se viene abajo.
Final malo: La situación empeora en minutos.

09:07 de la mañana

La gente empieza a avisar:

- “No puedo entrar al correo.”
- “El sistema va lentísimo…”
- “Todos mis archivos se han convertido en un nombre raro.”

De repente aparece un mensaje:
“Tus datos han sido cifrados. Para recuperarlos, paga.”

¿Qué decides?

Bien. La clave es reconocer antes de actuar. Activas el protocolo correcto: nadie toca nada sin instrucciones.

OPCIÓN B

“Paramos y avisamos: esto es un incidente serio”

09:15 de la mañana

Necesitas frenar el ataque, pero sin “apagar la empresa”.

¿Qué haces?

OPCIÓN A

Aislar equipos afectados (como cerrar una habitación en un incendio)

OPCIÓN B

Apagar todos los sistemas de la organización

09:15 de la mañana

Necesitas frenar el ataque, pero sin “apagar la empresa”.

¿Qué haces?

Actúas por pánico. Sí, el ataque se frena, pero también frenas el negocio entero.
Cuentas bancarias, almacén, facturación: *todo muerto*.
Final regular: se evita el desastre, pero el impacto empresarial es brutal.

OPCIÓN B

Apagar todos los sistemas de la organización

09:15 de la mañana

Necesitas frenar el ataque, pero sin “apagar la empresa”.

¿Qué haces?

OPCIÓN A

Aislar equipos afectados (como cerrar una habitación en un incendio)

Perfecto. Impides que el ataque se expanda sin paralizar toda la actividad.
Avanzas.

09:25 de la mañana

Es momento de coordinar a la organización.

¿A quién convocas?

OPCIÓN A

Solo al equipo técnico

OPCIÓN B

Al Comité de Crisis completo

09:25 de la mañana

Es momento de coordinar a la organización.

¿A quién convocas?

OPCIÓN A

Solo al equipo técnico

Insuficiente. Esto no es un problema solo de ordenadores.

Faltan Legal, Comunicación, Dirección y Negocio.

Decisiones cruciales no se tomarán a tiempo.

Final malo: el ataque técnico se resuelve, pero la reputación queda destrozada.

09:25 de la mañana

Es momento de coordinar a la organización.

¿A quién convocas?

Correcto. Esto es multidisciplinar:

- Dirección,
- Legal (por notificaciones y consecuencias regulatorias),
- Comunicación (empleados, proveedores, posibles filtraciones),
- TI y Ciberseguridad,
- Continuidad de negocio.

OPCIÓN B

Al Comité de Crisis completo

09:40 de la mañana

El correo no funciona. Teams tampoco. Necesitáis coordinaros ya.

¿Qué hacéis?

OPCIÓN A

Usar nuestros WhatsApp personales

OPCIÓN B

Usar el canal alternativo definido en el plan de crisis

09:40 de la mañana

El correo no funciona. Teams tampoco. Necesitáis coordinaros ya.

¿Qué hacéis?

OPCIÓN A

Usar nuestros WhatsApp personales

Rápido, sí, pero peligrosísimo.Puede filtrarse información sensible, y deja trazas difíciles de gestionar en auditorías o periciales.

Final regular.

09:40 de la mañana

El correo no funciona. Teams tampoco. Necesitáis coordinaros ya.

¿Qué hacéis?

Profesional, seguro y responsable.

Demuestra preparación real.

OPCIÓN B

Usar el canal alternativo definido en el plan de crisis

10:00 de la mañana

Empieza la pregunta que todo el mundo hace:

¿Pagamos el rescate?

OPCIÓN A

No. Usamos backups y reconstruimos

OPCIÓN B

Sí, para recuperar todo rápido

10:00 de la mañana

Empieza la pregunta que todo el mundo hace:

¿Pagamos el rescate?

Mala idea:

- No hay garantía de recuperación,
- Puede ser ilegal,
- Te convierte en objetivo,
- Suele haber copias alternativas o soluciones más seguras.

OPCIÓN B

Sí, para recuperar todo rápido

10:00 de la mañana

Empieza la pregunta que todo el mundo hace:

¿Pagamos el rescate?

OPCIÓN A

No. Usamos backups y reconstruimos

Decisión correcta. Pero solo si **los backups están probados y la infraestructura necesaria también**. (Empresas reales tardan días en restaurar porque… “las copias estaban bien pero las claves para usarlas estaban en un servidor cifrado”).

Avanzas.

11:30 de la mañana

Toca decidir qué restaurar primero.

¿Qué priorizas?

OPCIÓN A

El Sistemas de Nóminas

OPCIÓN B

El sistema que permite operar al negocio

11:30 de la mañana

Toca decidir qué restaurar primero.

¿Qué priorizas?

OPCIÓN A

El Sistemas de Nóminas

Tentador, pero no crítico.

No es la prioridad Nº1.

11:30 de la mañana

Toca decidir qué restaurar primero.

¿Qué priorizas?

Exacto.

La prioridad es **volver a trabajar**, aunque sea en modo degradado.

Has tomado el camino correcto.

OPCIÓN B

El sistema que permite operar al negocio

17:00 de la tarde: Final bueno

Aunque la mañana ha sido un caos, tus decisiones han permitido:

- ✓ **Contener el ataque**
- ✓ **Coordinar equipos**
- ✓ **Evitar daños reputacionales innecesarios**
- ✓ **Cumplir con regulación**
- ✓ **Mantener la operación básica**
- ✓ **Planificar una recuperación controlada**

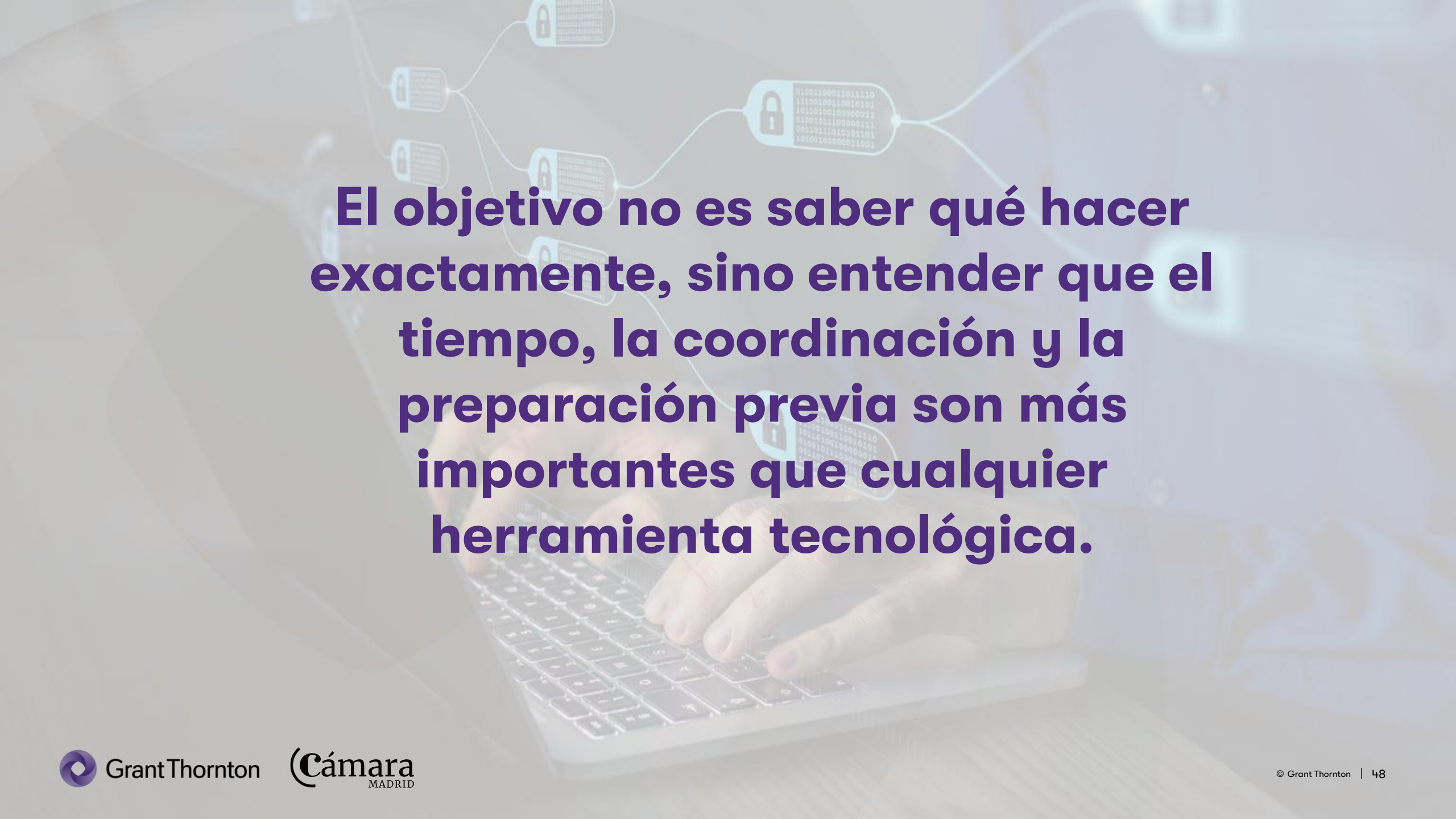
Te acaban de cifrar los sistemas, ¿qué haces ahora?

Paso a paso, qué debe hacer una organización:

1. Mantener la calma
2. Aislar, no apagar
3. Activar al Comité de Crisis (la “sala de mando”)
4. Decisiones rápidas
5. ¿Pagamos el rescate?
6. Recuperar la actividad
7. Aprender del incidente

Grant Thornton

Cámara MADRID



El objetivo no es saber qué hacer exactamente, sino entender que el tiempo, la coordinación y la preparación previa son más importantes que cualquier herramienta tecnológica.

Grant Thornton

Cámara MADRID

Primeras horas tras un ciberataque: respuestas rápidas y efectivas sin comprometer el negocio

11 de marzo

GrantThornton.es