7 CLAVES PARA BLINDAR TU CLÍNICA FRENTE A UN CIBERATAQUE

GUÍA PRÁCTICA DE CIBERSEGURIDAD PARA CLÍNICAS Y HOSPITALES

Cris Digital

Este manual esencial es la continuación práctica del artículo '**Cómo actúa un ciberatacante para atacar una clínica**'.

Escanea el QR para leerlo completo o haz click aquí .

Índice

Introducción
- Por qué las clínicas son un objetivo
- Casos reales en el sector salud

Fase 1 – Reconocimiento
Fase 2 – Acceso inicial
Fase 3 – Consolidación del acceso
Fase 4 – Movimiento lateral
Fase 5 – Exfiltración y secuestro
Fase 6 – Ataque final
Fase 7 – Monetización y extorsión

Conclusión
- A quién recurrir
- La importancia de un responsable de ciberseguridad

MEDIDAS PRÁCTICAS PARA ANTICIPARSE A CADA FASE DE UN ATAQUE DIGITAL

En el artículo que acabas de leer hemos visto las 7 fases que recorre un atacante para entrar en una clínica: observar lo que está expuesto, moverse entre sistemas, robar información y chantajear. Este mini e-book es el siguiente paso: aquí encontrarás cómo puedes frenar cada una de esas fases con medidas prácticas y adaptadas a tu realidad.

¿Por qué tu clínica es hoy un objetivo tan atractivo?

1. Porque los datos médicos tienen un valor altísimo en el mercado negro, mucho más que una tarjeta bancaria.
2. Porque el servicio de salud no puede detenerse: ni un hospital ni una clínica pueden cerrar por un día sin poner en riesgo vidas, lo que genera más presión para pagar un rescate.
3. Porque muchos centros trabajan con recursos limitados en ciberseguridad y mantienen tecnologías antiguas o mal configuradas.

No se trata de un temor hipotético. Según el INCIBE, el sector salud concentra ya más del 40 % de los incidentes graves de ciberseguridad en Europa. Y la Comisión Europea ha tenido que lanzar un Plan de Acción específico para hospitales dentro de su estrategia de ciberseguridad.

La idea central es clara: la protección empieza cuando aceptas que tu clínica también está en el punto de mira. Prepararte no significa convertirte en experto en tecnología, sino tomar decisiones inteligentes: diferenciar qué puede prevenir tu propio equipo (por ejemplo, en el uso de correos, enlaces o redes sociales) y qué debe delegarse en un responsable de ciberseguridad.

Ese responsable no es el informático que hace copias de seguridad, sino la persona encargada de asegurar que todo está configurado correctamente, sin brechas que un atacante pueda aprovechar. Contar con esa figura es clave para reducir riesgos, fortalecer la confianza de tus pacientes y marcar la diferencia entre ser vulnerable o estar preparado.

Nota importante

A lo largo de este manual esencial menciono ***"al responsable de ciberseguridad".***

Si tu clínica no cuenta con uno, verás que a lo largo del texto se pone de relieve ***la importancia de tener a alguien que asuma estas tareas.*** *No es imprescindible que sea un empleado a tiempo completo: puedes apoyarte en un profesional o servicio externo especializado.*

Lo fundamental es contar con una persona de referencia que pueda guiar, coordinar y aplicar las medidas de protección.

Introducción

Un patrón que se repite

En los últimos años, clínicas y hospitales de todo el mundo —**grandes y pequeños**— han sido blanco de ataques que siguen un patrón muy parecido. Aunque los grandes titulares suelen referirse a hospitales con cientos de camas, los ataques también afectan a clínicas más reducidas, y muchas veces con impactos devastadores.

El análisis de estos casos revela que l**os ataques avanzan por fases muy similares:** primero la observación y el reconocimiento, después el acceso inicial, y finalmente la propagación y el secuestro de sistemas.

Ese mismo patrón es el que vas a ver explicado en este minibook, con medidas prácticas que puedes aplicar en tu clínica.

Cada vez se detectan más incidentes en el sector salud. A continuación, te comparto algunos de los casos más relevantes de los últimos años y en qué fase de esta guía se analizan.

Casos reales en el sector salud

- ***España, 2025 –*** *Hospital Los Madroños (Madrid): Ataque del grupo Qilin: cifrado de sistemas y publicación de datos en la dark web.* ***Explicado en la Fase 6 (Exfiltración/bloqueo) y la Fase 7 (Extorsión).***

- *Alemania, 2020 – Hospital Universitario de Düsseldorf: Ransomware que paralizó el hospital tras el uso de credenciales robadas sin detección de anomalías.* ***Explicado en la Fase 3 (Acceso inicial) y la Fase 4 (Consolidación/persistencia).***

- *Irlanda, 2021 – Health Service Executive (HSE): Ataque del grupo Conti que paralizó la sanidad nacional durante semanas.* ***Explicado en la Fase 5 (Movimiento lateral) y la Fase 6 (Exfiltración de datos/bloqueo).***

- *Francia, 2022 – Centre Hospitalier Sud Francilien (CHSF): Ransomware de LockBit con bloqueo de sistemas y filtración de datos clínicos.* ***Explicado en la Fase 4 (Consolidación) y la Fase 6 (Exfiltración de datos).***

- *Francia, 2022 – Hospital André Mignot (Versalles): Ciberataque que obligó a trasladar pacientes y suspender cirugías.* ***Explicado en la Fase 6 (Impacto final).***

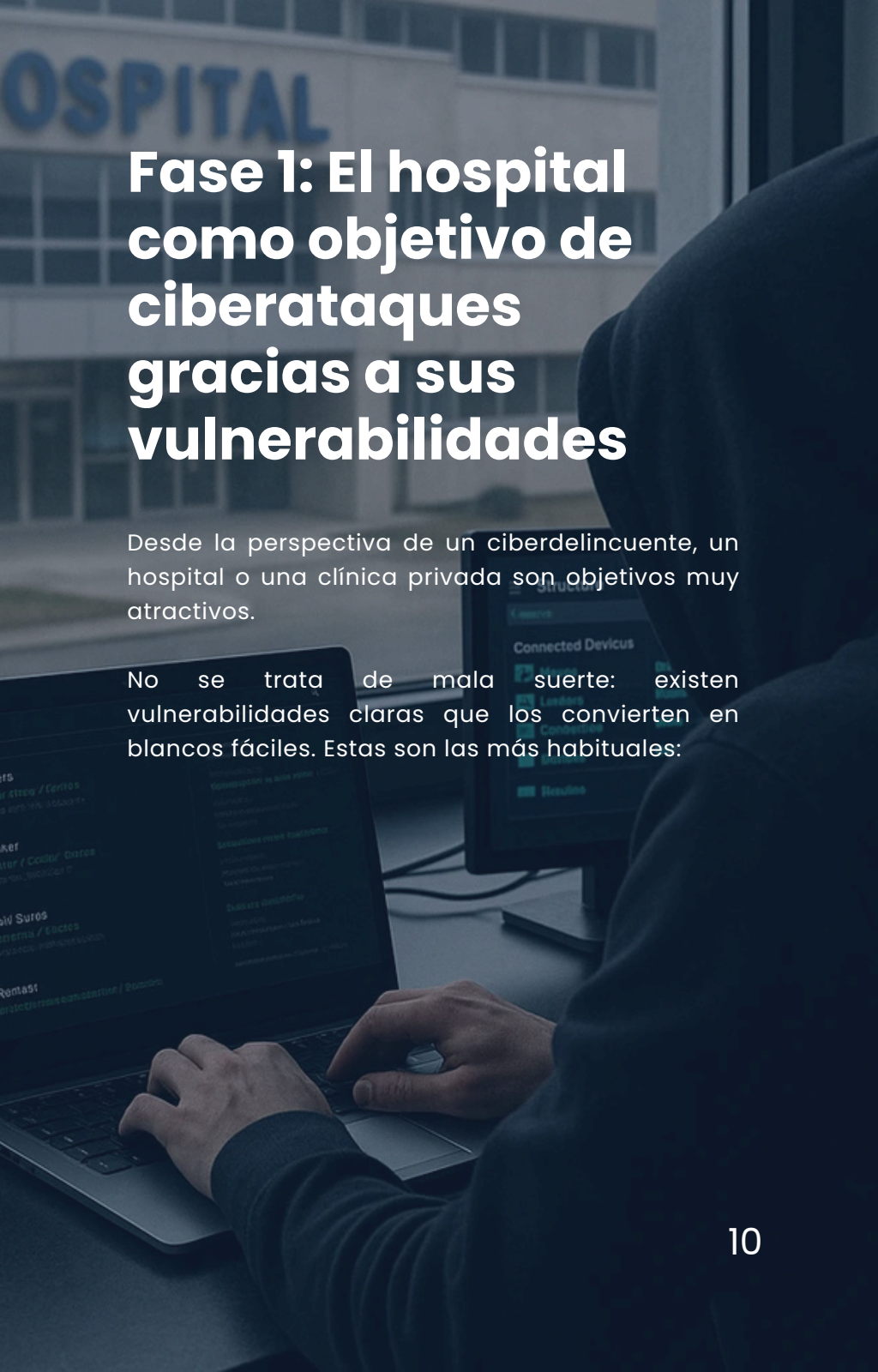
- *España, 2023 – Hospital Clínic de Barcelona: Ataque del grupo RansomHouse con propagación de ransomware por falta de autenticación multifactorial. Explicado en la* ***Fase 5 (Movimiento lateral) y la Fase 6 (Exfiltración/bloqueo).***

- *Francia, 2024 – Hospital Simone Veil (Cannes): Publicación de decenas de gigas de datos clínicos tras un ataque de LockBit. Explicado en la* ***Fase 6 (Exfiltración) y la Fase 7 (Extorsión/monetización).***

- *Reino Unido, 2017 – NHS (WannaCry): Colapso en numerosos hospitales tras la propagación del ransomware WannaCry.* ***Explicado en la Fase 3 (Acceso inicial) y en la Fase 5 (Movimiento lateral).***

- *Alemania/Suiza, 2025 – Red hospitalaria AMEOS: Acceso no autorizado que obligó a apagar sistemas en varios centros y confirmó exposición de datos. Explicado en la* ***Fase 5 (Movimiento lateral) y la Fase 6 (Exfiltración).***

Como ves, los incidentes no ocurren de golpe: avanzan paso a paso siguiendo un patrón.
A continuación descubrirás cada fase del ataque y, lo más importante, qué puedes hacer en tu clínica para detenerlo a tiempo.



Fase 1: El hospital como objetivo de ciberataques gracias a sus vulnerabilidades

Desde la perspectiva de un ciberdelincuente, un hospital o una clínica privada son objetivos muy atractivos.

No se trata de mala suerte: existen vulnerabilidades claras que los convierten en blancos fáciles. Estas son las más habituales:

1. El valor de los datos

Los historiales médicos contienen información muy sensible (nombre, dirección, número de la Seguridad Social, enfermedades, tratamientos, etc.). En los mercados ilegales estos datos se venden a muy buen precio, incluso por encima de los datos bancarios.

2. La urgencia del servicio médico

Un hospital o clínica no puede detener su actividad ni por horas ni por días. Cuando los sistemas fallan, la presión para resolverlo rápidamente es enorme, y eso hace que pagar un rescate sea más probable.

3. Falta de actualizaciones en los sistemas

Muchos equipos y programas sanitarios no reciben las actualizaciones de seguridad que corrigen fallos conocidos. Si esos fallos siguen abiertos, un atacante los aprovechará para entrar.

4. Falta de personal especializado en seguridad informática

En la mayoría de los centros no existe un equipo dedicado exclusivamente a proteger los sistemas. El personal de informática suele centrarse en que todo funcione, pero no en detectar y prevenir ataques. Esa brecha deja a la clínica desprotegida.

5. Muchos dispositivos conectados

En un hospital hay decenas o cientos de dispositivos con acceso a Internet: ordenadores, impresoras, cámaras, servidores e incluso equipos médicos. Cada uno de ellos es una puerta potencial de entrada. Si no está bien configurado, puede ser usado por un atacante para llegar al resto de la red.

Resultado de esta fase

Aceptar que tu clínica reúne estas condiciones no es un signo de debilidad, sino el primer paso para protegerla. Lo que hoy hace atractiva a tu clínica para un ciberdelincuente es exactamente lo que puedes empezar a blindar.

Fase 2: Cómo reducir tu huella digital y cerrar la puerta al reconocimiento externo

En esta etapa, el atacante aún no ha entrado en tu clínica: solo observa desde fuera.

Su objetivo es recopilar toda la información posible para preparar un ataque a medida. La buena noticia es que está en tu mano decidir qué muestras y qué escondes: cuanto menos dejes a la vista, menos material tendrá el atacante para preparar su ataque.

1. Información pública: comunica sin regalar tu inventario

- **Qué hacer en la clínica**: define una política de comunicación segura. Esto significa que cualquier nota de prensa, post en redes o documento público se revisa antes de publicar para asegurarse de que no contiene:

Un error habitual en clínicas es publicar en redes fotos de las nuevas instalaciones con pantallas encendidas detrás, donde se ve información sensible sin querer.

  - Nombres concretos de software o proveedores
  - Capturas de pantallas internas
  - Datos de personal clave como correos directos de dirección o gerencia.

  En lugar de decir "hemos implantado el sistema X de la empresa Y", comunícalo así: "hemos mejorado la atención digitalizando historiales".

- **Responsable de ciberseguridad:** validar que toda comunicación externa pasa por un checklist apropiado que evite fugas de información sensible o pistas técnicas que un atacante pueda aprovechar.

- **Por qué funciona**: reduces el riesgo de exfiltración de información crítica y eliminas desde el principio el material que un atacante podría usar para suplantar o preparar un phishing convincente.

2. Dispositivos accesibles desde Internet: no dejes ventanas abiertas

- **Qué hacer en la clínica**: pide un informe de exposición externa cada trimestre. Esto revisa qué dispositivos de tu clínica están visibles desde fuera (cámaras, impresoras, equipos médicos, servidores).

- **Responsable de ciberseguridad**: garantizar que estos equipos nunca sean accesibles de forma directa desde Internet. Todo acceso remoto debe pasar por VPN + doble factor, y los equipos médicos deben estar en una red separada del resto de sistemas administrativos.

- **Por qué funciona**: si alguien escanea desde fuera, no encontrará ni una sola ventana abierta.

Glosario

- **VPN (Red Privada Virtual)**: es como un túnel seguro para que solo quien tenga la llave pueda entrar desde fuera.
- **Doble factor de autenticación (2FA)**: además de la contraseña, se pide una segunda prueba, como un código en el móvil. Así, aunque roben la clave, no podrán entrar.
- **Segmentación de red**: significa separar los equipos médicos del resto (por ejemplo, la parte administrativa). De este modo, si un atacante entra en un ordenador de oficina, no puede saltar directamente a un aparato médico.

3. Documentos mal compartidos: que lo interno se quede interno

- **Qué hacer en la clínica**: centraliza la gestión documental en una plataforma corporativa (SharePoint, Nextcloud) y elimina la opción de enlaces públicos sin control. Educa a tu personal para que nunca suba documentos internos con permisos abiertos.

- **Responsable de ciberseguridad**: configurar la nube corporativa para que ningún archivo pueda indexarse en buscadores y auditar periódicamente los accesos.

- **Por qué funciona**: evitas que un simple despiste acabe convirtiéndose en un regalo con información técnica y listados internos.

4. Correos filtrados: detecta la llave perdida antes que ellos

- **Qué hacer en la clínica**: monitorear mensualmente si correos del dominio aparecen en bases de datos filtradas. Si ocurre, obliga al cambio inmediato de contraseña.

- **Responsable de ciberseguridad**: implantar un gestor corporativo de contraseñas y habilitar doble factor en correo, software clínico y VPN.

- **Por qué funciona**: aunque una contraseña antigua circule en foros criminales, ya no sirve para abrir tu puerta.

5. Huella digital del personal: forma parte de la defensa

- **Qué hacer en la clínica**: sensibiliza a tu equipo sobre lo que publican en redes sociales. Un simple post en LinkedIn celebrando la implantación de un software o una foto con el uniforme puede dar a un atacante pistas valiosas.

- **Responsable de ciberseguridad**: elaborar una guía rápida de buenas prácticas para redes sociales: qué se puede compartir y qué no.

- **Por qué funciona**: reduces el riesgo de que la propia plantilla, sin saberlo, regale información que facilite la ingeniería social.

6. Monitorización activa: vigila lo qué ya está expuesto

- **Qué hacer en la clínica**: solicita informes periódicos de huella digital (*rastro de información pública de tu clínica en internet, como documentos, correos o datos visibles*) a tu responsable de ciberseguridad o proveedor especializado.

- **Responsable de ciberseguridad**: utilizar herramientas especializadas que rastrean buscadores, foros y bases de datos si hay documentos, subdominios o dispositivos del dominio expuestos.

- **Por qué funciona**: no basta con prevenir; también hay que saber si algo ya ha salido fuera para poder reaccionar a tiempo.

Al aplicar las medidas de la Fase 2, esto es lo que consigues

Tomando estas medidas, el ciberdelincuente no encontrará material suficiente para preparar un ataque a medida. Y si no puede personalizar su estrategia en esta fase, no tendrá cómo avanzar a la siguiente. En la práctica, lo más probable es que descarte tu clínica y dirija sus esfuerzos hacia otro centro menos protegido, uno que no haya aplicado estas precauciones.

Fase 3: El primer contacto (acceso inicial)

Supongamos que tu clínica no aplicó las medidas que te he recomendado en la Fase 2. El atacante ya consiguió superar esa etapa y ahora llega al primer contacto real: es el momento en el que intenta entrar en tu sistema o en el día a día de tu personal.

Aquí es donde el error humano suele abrir la puerta. Un clic en un correo, una llamada atendida sin sospecha, una contraseña débil o un acceso mal configurado pueden ser suficientes. Pero si tu clínica está preparada en esta fase, el atacante se queda bloqueado.

1. Correos engañosos (phishing)

- **Qué hacer en la clínica**: formar al personal para que sepa identificar correos sospechosos y establecer un protocolo claro para reportar cualquier correo extraño de inmediato. El dueño o coordinador debe asegurarse de que toda la plantilla recibe esta formación periódicamente.

- **Responsable de ciberseguridad**: lanzar simulaciones de phishing varias veces al año para comprobar si el personal sabe reaccionar, además de reforzar los filtros de correo y bloquear dominios maliciosos conocidos.

- **Por qué funciona**: el phishing explota el error humano. Con formación y simulaciones, reduces al mínimo la posibilidad de que alguien abra la puerta sin darse cuenta.

2. Mensajes o llamadas fraudulentas (smishing y vishing)

- **Qué hacer en la clínica**: establecer una regla clara de que nadie pedirá contraseñas por teléfono ni por SMS. Define un protocolo de verificación antes de cumplir cualquier instrucción sospechosa y utiliza, si es necesario, una contraseña verbal interna para validar llamadas legítimas..

- **Responsable de ciberseguridad**: configurar alertas ante intentos de acceso remoto no autorizados y mantener registros de llamadas o tickets que sirvan para detectar patrones sospechosos.

- **Por qué funciona**: cuando el personal sabe que ninguna llamada legítima pedirá credenciales, la mayoría de estos intentos se bloquean al instante.

3. Uso de contraseñas robadas

- **Qué hacer en la clínica**: prohibir la reutilización de contraseñas entre cuentas personales y profesionales, y hacer cambios de contraseña cada dos o tres meses.

- **Responsable de ciberseguridad**: implantar un gestor corporativo de contraseñas y activar multifactor (MFA) en todos los accesos críticos.

- **Por qué funciona**: aunque una contraseña circule en foros criminales, el multifactor evita que pueda abrir ninguna puerta.

4. Accesos remotos mal protegidos

- **Qué hacer en la clínica**: contar con un checklist de seguridad que el dueño revise periódicamente con su responsable de ciberseguridad. Entre las preguntas clave:
  - ¿Existen accesos remotos abiertos a Internet sin protección?
  - ¿Se han cambiado las contraseñas de administrador recientemente?
  - ¿Se han hecho simulaciones de phishing en los últimos meses?

- **Responsable de ciberseguridad**: cerrar todos los puertos innecesarios, reforzar accesos con firewalls y multifactor, y revisar la configuración de proveedores externos que acceden al sistema.

- **Por qué funciona**: blindar accesos remotos corta una de las rutas de entrada más habituales del ransomware en el sector salud.

5. Dispositivos físicos infectados (USB u otros)

- **Qué hacer en la clínica**: establecer una política clara que prohíba conectar dispositivos externos no autorizados en los equipos de la clínica.

- **Responsable de ciberseguridad**: configurar los equipos para que los USB no se ejecuten automáticamente y monitorizar los registros de conexión de dispositivos.

- **Por qué funciona**: evitas que un simple gesto de curiosidad acabe en una intrusión silenciosa.

Al aplicar las medidas de la Fase 3, esto es lo que consigues

Si aplicas estas medidas, el atacante puede llegar hasta la puerta, pero no logrará entrar. Sin correos efectivos, sin contraseñas válidas, sin accesos remotos inseguros y con una política estricta sobre dispositivos, se queda bloqueado en el primer contacto. Y lo más importante: al no conseguir una entrada silenciosa, probablemente abandone y busque otra clínica menos preparada.

Fase 4: El atacante se asegura de poder quedarse dentro (consolidación)

Supongamos que el atacante ha conseguido pasar la Fase 3 porque no has tomado las medidas que te he recomendado. En ese momento ya estaría dentro de tu clínica, aunque todavía no haya hecho ruido, y su prioridad no sería atacar de inmediato, sino garantizar que puede mantenerse dentro sin ser expulsado. Para lograrlo, en esta fase busca instalar programas ocultos, conseguir permisos de administrador, crear cuentas falsas, explorar la red con calma y borrar sus huellas.

1. Cómo detectar y bloquear los programas ocultos y puertas traseras que instala el atacante

- **Qué hacer en la clínica**: tu equipo debe estar formado para reportar cualquier comportamiento extraño en los ordenadores: lentitud repentina, ventanas que se abren solas, programas desconocidos o desconexiones frecuentes. El personal formado es la primera línea de defensa

- **Responsable de ciberseguridad**: instalar un sistema de protección avanzado (EDR, Endpoint Detection & Response) que no solo bloquee malware, sino que alerte sobre procesos sospechosos o conexiones no autorizadas. Realizar auditorías periódicas para comprobar que no se han instalado programas ocultos ni puertas traseras.

- **Por qué funciona**: : si se detecta un programa sospechoso en los primeros momentos, se elimina la puerta de entrada secreta que el atacante necesita para volver a entrar.

2. Cómo impedir que el atacante consiga permisos de administrador en tus sistemas

- **Qué hacer en la clínica**: establece la regla de que nadie trabaje con cuentas de administrador en el día a día. Los empleados deben usar cuentas con permisos mínimos, y solo un número muy reducido de personas puede tener acceso a privilegios altos.

- **Responsable de ciberseguridad**: aplicar el principio de mínimo privilegio en todos los sistemas, gestionar las contraseñas de administrador con herramientas seguras y auditar de forma regular los accesos privilegiados.

- **Por qué funciona**: aunque el atacante entre en una cuenta de usuario, si no puede escalar a administrador, se queda atascado sin capacidad de controlar ni borrar información crítica.

3. Cómo evitar que el atacante cree cuentas ocultas y se quede sin que lo notes

- **Qué hacer en la clínica:** define un protocolo para que el personal avise si detecta cuentas nuevas en los equipos o accesos extraños que no corresponden a usuarios reales.

- **Responsable de ciberseguridad:** revisar periódicamente todas las cuentas activas y las tareas programadas en los equipos. Configurar alertas que salten cuando se crea un nuevo usuario con permisos altos o cuando se cambian políticas del sistema sin autorización.

- **Por qué funciona:** si bloqueas la persistencia, el atacante pierde el acceso tras un reinicio o un cambio de contraseña.

4. Cómo frenar al atacante cuando intenta explorar la red de tu clínica (incluyendo móviles del personal y pacientes)

- **Qué hacer en la clínica**: no todos los equipos necesitan acceso a todos los sistemas. Limita qué ordenadores y dispositivos pueden conectarse a cada parte de la red y establece normas claras: por ejemplo, un ordenador administrativo no debería llegar a un servidor clínico. Y, sobre todo, controla también los móviles del personal y los pacientes: estos nunca deben conectarse a la red corporativa, sino a una red Wi-Fi separada.

- **Responsable de ciberseguridad:** segmentar la red en distintas zonas (administración, equipos médicos, sistemas clínicos, Wi-Fi invitados) y usar firewalls internos que impidan a un atacante moverse libremente. Además, debe revisar periódicamente qué dispositivos están conectados y con qué permisos.

- **Por qué funciona**: cuando los móviles del personal y los de los pacientes se mantienen en redes separadas, se elimina una de las vías más frecuentes para que el atacante explore la red y detecte vulnerabilidades.

5. Cómo detectar al atacante antes de que borre sus huellas

- **Qué hacer en la clínica**: fomenta una cultura de alerta: cualquier cosa rara debe reportarse. Aunque parezca un detalle menor, puede ser la clave para descubrir una intrusión.

- **Responsable de ciberseguridad**: implementar un SIEM (*una herramienta que centraliza y vigila toda la actividad de los sistemas para detectar comportamientos extraños*) que centralice los registros de actividad y genere alertas de comportamientos anómalos (cambios en logs, nombres de archivos modificados, accesos fuera de horario).

- **Por qué funciona**: cuanto antes se detecta un intento de ocultación, menos margen tiene el atacante para seguir moviéndose en silencio.

- *Si quieres, escríbeme y te enviaré una guía práctica donde explico cómo gestionar de forma segura los dispositivos del personal y los pacientes (móviles, tablets o Wi-Fi de invitados) para que no se conviertan en una puerta de entrada al sistema.*

Al aplicar las medidas de la Fase 4, esto es lo que consigues

Si aplicas estas medidas, el atacante puede haber entrado, pero no logrará quedarse. No podrá instalar programas ocultos, ni conseguir permisos de administrador, ni crear cuentas falsas, ni moverse por la red sin ser detectado. Y cuando no consigue consolidar su acceso, tarde o temprano será expulsado. Eso convierte a tu clínica en un entorno mucho más difícil de explotar y lo empuja a buscar un objetivo más vulnerable.

Fase 5: El atacante empieza a moverse por la red (movimiento lateral)

Supongamos que el atacante ha conseguido superar la Fase 4 porque no aplicaste las medidas que te he recomendado. En ese caso, ya está dentro de tu clínica y su objetivo ahora es ampliar su control. Esta fase consiste en moverse por la red de forma silenciosa, saltando de un ordenador a otro, probando nuevas contraseñas y buscando dónde están los sistemas y datos más valiosos.

Es como si estuviera en tu clínica con una llave maestra: recorriendo los pasillos, abriendo las consultas, mirando para localizar dónde guardas lo más importante. Cada puerta que abre sin ser visto lo acerca más a su golpe final.

1. Cómo evitar que el atacante salte de un ordenador a otro

- **Qué hacer en la clínica**: establece reglas claras de uso: cada empleado debe acceder solo a lo que realmente necesita para su trabajo, y nunca compartir contraseñas con compañeros "por rapidez". El personal debe entender que un acceso innecesario es una puerta abierta de más.

- **Responsable de ciberseguridad**: aplicar la segmentación de red y configurar firewalls internos que impidan al atacante moverse libremente de un ordenador a otro. Revisar periódicamente los permisos de acceso y cerrar cualquier conexión que no sea imprescindible.

- **Por qué funciona**: si la red está segmentada y los permisos bien gestionados, el atacante se queda encerrado en el primer equipo al que ha entrado y no puede expandirse.

2. Cómo impedir que el atacante localice los sistemas más valiosos

- **Qué hacer en la clínica**: define junto a tu responsable qué sistemas son críticos (bases de datos de pacientes, sistemas financieros, servidores de imagen médica) y limita quién puede acceder a ellos. A nivel de personal, explica que los datos clínicos solo deben consultarse cuando es estrictamente necesario, no como costumbre.

- **Responsable de ciberseguridad**: aplicar el principio de mínimo privilegio en los servidores críticos y monitorizar de forma continua quién accede a ellos. Instalar alertas que se activen cuando un usuario sin perfil autorizado intente entrar en estos sistemas.

- **Por qué funciona**: cuanto más restringido está el acceso, más difícil es que el atacante pueda llegar a los “tesoros” de tu clínica.

3. Cómo bloquear al atacante cuando intenta robar o reutilizar contraseñas

- **Qué hacer en la clínica**: establece como norma que las contraseñas deben cambiarse cada dos o tres meses, que no se reutilicen y que nunca se guarden en archivos de texto o notas. Además, el personal debe saber reportar cualquier intento de solicitud de credenciales sospechoso.

- **Responsable de ciberseguridad**: usar un gestor corporativo de contraseñas y activar el doble factor de autenticación en todos los accesos críticos. Revisar periódicamente si alguna credencial del dominio ha aparecido filtrada en Internet.

- **Por qué funciona**: aunque el atacante intente capturar contraseñas con programas maliciosos, el doble factor y la rotación frecuente bloquean su utilidad.

4. Cómo detectar si el atacante se disfraza de usuario legítimo

- **Qué hacer en la clínica:** refuerza la cultura de alerta: un empleado debe comunicar si observa accesos sospechosos en horarios en los que él no estaba trabajando o si recibe notificaciones de inicio de sesión que no reconoce.

- **Responsable de ciberseguridad:** implantar un sistema de monitorización de comportamiento de usuarios como UEBA (*una herramienta que analiza el comportamiento de los usuarios para detectar accesos extraños o fuera de lo normal*) que detecte anomalías, como un médico que de repente accede a servidores de administración o un usuario que empieza a entrar de madrugada.

- **Por qué funciona**: aunque el atacante intente camuflarse con cuentas reales, los patrones de comportamiento dejan señales que pueden detectarse.

Al aplicar las medidas de la Fase 5, esto es lo que consigues

Si aplicas estas medidas, el atacante no podrá moverse por tu clínica como por un pasillo abierto. No logrará saltar de un ordenador a otro, ni llegar a los sistemas más valiosos, ni aprovechar credenciales robadas, ni camuflarse como un usuario legítimo. Y si no puede expandirse lateralmente, pierde la oportunidad de preparar el gran golpe: robar datos, bloquear sistemas o pedir un rescate.

Fase 6: El hospital en jaque (secuestro digital y filtración de datos)

Supongamos que el atacante ha conseguido avanzar hasta aquí porque no aplicaste las medidas que te he recomendado en la Fase 5. Después de moverse por la red de tu clínica y localizar lo más valioso, ahora ya no se limita a explorar: entra en acción. Su objetivo en esta fase es claro: llevarse datos en secreto y/o bloquear sistemas para pedir un rescate.

Es como si el intruso que tenía la llave maestra hubiese recorrido todos los pasillos de tu clínica, hubiese encontrado la caja fuerte y ahora se dispusiera a vaciarla o a cerrarla con su propio candado, dejándote sin acceso a lo que necesitas para trabajar.

1. Cómo evitar la exfiltración de datos confidenciales

- **Qué hacer en la clínica**: tu personal debe estar formado para reconocer comportamientos extraños en los sistemas: archivos que desaparecen, correos de pacientes que reportan haber recibido documentos que no deberían, o copias de seguridad que no se pueden abrir. Cualquier anomalía debe ser reportada de inmediato.

- **Responsable de ciberseguridad**: implantar sistemas de DLP (Data Loss Prevention, *herramientas que evitan que información confidencial salga de la clínica sin autorización*) y monitorización del tráfico de red, que detecten cuando se intenta extraer gran volumen de datos o información sensible disfrazada como tráfico normal. Revisar también periódicamente qué datos salen fuera de la organización y con qué destino.

- **Por qué funciona**: si detectas la salida de información en tiempo real, puedes cortar la conexión y evitar que los historiales médicos o datos financieros acaben en la dark web.

2. Cómo impedir que el atacante bloquee sistemas críticos (ransomware)

- **Qué hacer en la clínica**: exige a tu equipo que las copias de seguridad no estén nunca conectadas a la red principal. No basta con tener backups: deben estar aislados (offline o en un entorno separado). Haz simulacros periódicos de recuperación para comprobar que realmente funcionan. Y establece un protocolo claro: en caso de bloqueo, no pagar nunca un rescate sin consultar con expertos y autoridades.

- **Responsable de ciberseguridad**: mantener las copias de seguridad en entornos aislados, controlar los accesos con doble factor de autenticación y revisar regularmente que los sistemas de backup no tengan conexiones abiertas a la red clínica.

- **Por qué funciona**: aunque el atacante consiga cifrar servidores, si las copias están aisladas podrás restaurar la actividad y mantener la continuidad sin ceder al chantaje.

3. Cómo reducir el impacto de una filtración o un bloqueo

- **Qué hacer en la clínica**: define un plan de respuesta a incidentes y ensáyalo con tu equipo: ¿Qué pasos seguir si un sistema se bloquea?, ¿a quién se avisa primero?, ¿Cómo se garantiza la atención a pacientes en paralelo?

- **Responsable de ciberseguridad**: coordinar simulacros de ataque, mantener canales de comunicación seguros y preparar un protocolo de notificación a autoridades y pacientes, en caso de que datos se vean comprometidos.

- **Por qué funciona:** un ataque mal gestionado multiplica el daño. Con un plan claro y ensayado, tu clínica puede seguir funcionando mientras los expertos controlan la situación.

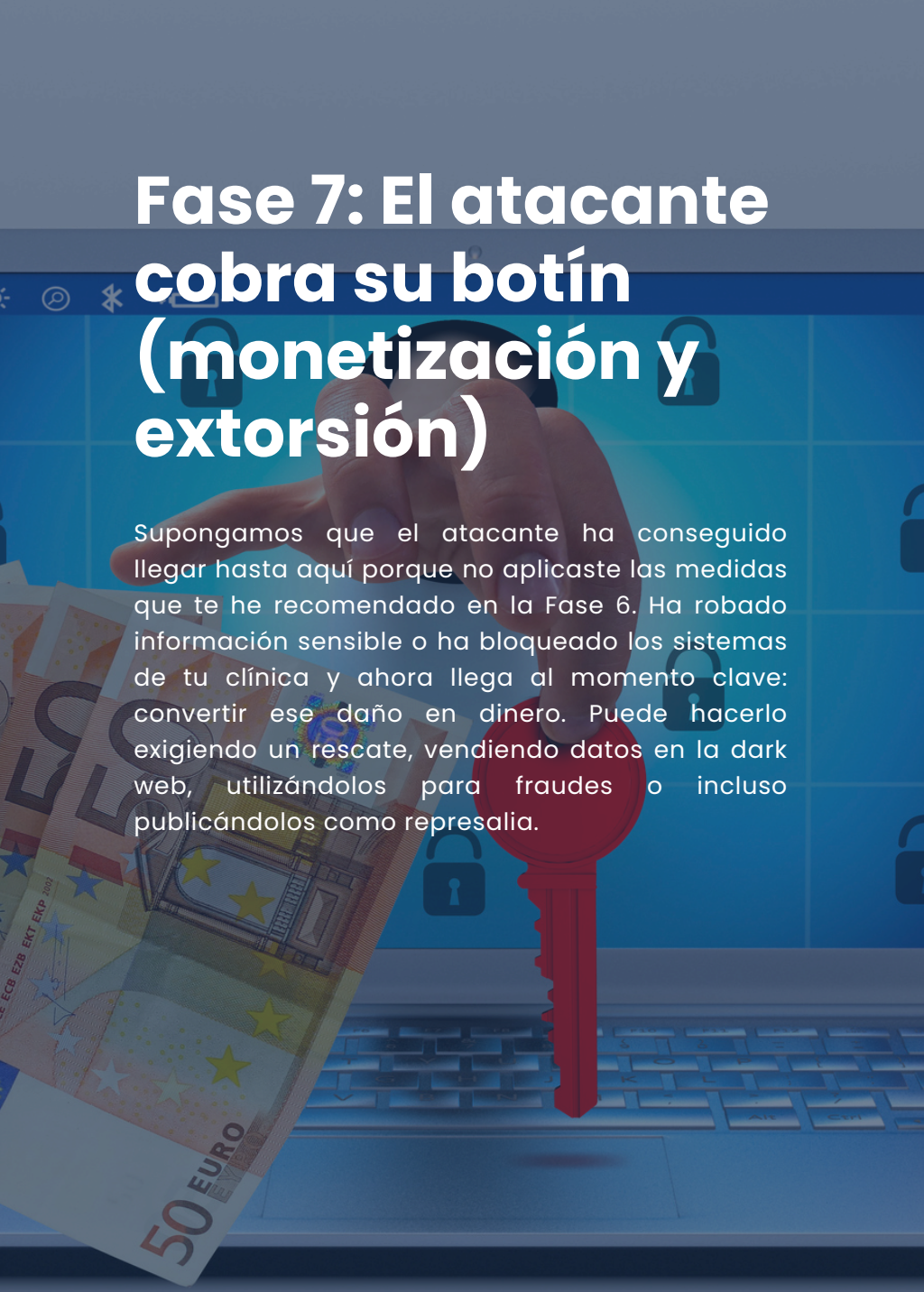
Al aplicar las medidas de la Fase 6, esto es lo que consigues

Si tu clínica llega a esta fase con las defensas activas, el atacante puede haber encontrado la caja fuerte, pero no podrá abrirla ni llevársela. No logrará exfiltrar historiales médicos ni bloquear los sistemas esenciales, porque tus copias de seguridad estarán protegidas, tu personal sabrá cómo actuar y tu responsable de ciberseguridad tendrá herramientas para cortar la fuga a tiempo.

Y cuando un atacante ve que robar o cifrar tus datos no es posible, pierde su ventaja de presión. Lo más probable es que abandone e intente un objetivo menos preparado. En otras palabras: puede haber llegado muy lejos, pero no conseguirá doblegar a tu clínica.

Fase 7: El atacante cobra su botín (monetización y extorsión)

Supongamos que el atacante ha conseguido llegar hasta aquí porque no aplicaste las medidas que te he recomendado en la Fase 6. Ha robado información sensible o ha bloqueado los sistemas de tu clínica y ahora llega al momento clave: convertir ese daño en dinero. Puede hacerlo exigiendo un rescate, vendiendo datos en la dark web, utilizándolos para fraudes o incluso publicándolos como represalia.



1. Cómo reducir el impacto de una extorsión directa

- **Qué hacer en la clínica**: ten un protocolo claro que indique a la dirección cómo actuar: nunca pagar un rescate sin consultar con expertos, notificar inmediatamente a las autoridades y comunicar de forma transparente al personal que tiene que gestionar la crisis. La comunicación honesta evita rumores y pérdida de confianza interna.

- **Responsable de ciberseguridad**: preservar evidencias digitales para ayudar a la investigación, coordinar la contención técnica y contactar de inmediato con INCIBE-CERT (Computer Emergency Response Team, cada país tiene el suyo; en España corresponde a INCIBE-CERT) y con las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional o Guardia Civil).

- **Por qué funciona**: no pagar evita financiar al atacante y reduce la probabilidad de que vuelva a extorsionarte. Además, actuar con rapidez limita la duración de la interrupción y la presión económica.

2. Cómo adelantarte a la venta de datos en mercados clandestinos

- **Qué hacer en la clínica**: prepara un plan de comunicación externa para pacientes y colaboradores, explicando qué información puede haberse visto comprometida y qué medidas deben tomar (cambio de contraseñas, alerta de fraudes, etc.). Esto protege la confianza y demuestra responsabilidad.

- **Responsable de ciberseguridad:** monitorizar foros de la dark web y redes clandestinas para detectar si datos de la clínica aparecen a la venta. Coordinarse con empresas especializadas en ciberinteligencia para tener visibilidad de lo que ocurre fuera de la clínica. El responsable puede cubrir lo básico, pero la detección profunda requiere apoyo externo.

- **Por qué funciona**: si reaccionas rápido cuando aparecen datos robados, puedes limitar el daño reputacional, proteger a tus pacientes y cumplir con la normativa de notificación (RGPD).

3. Cómo evitar que los datos se usen para otros fraudes

- **Qué hacer en la clínica:** tu clínica debe ser la fuente oficial de información. Ten preparado un manual de comunicación y un boletín ya listo para enviar a pacientes y personal en caso de filtración. Explica qué riesgos existen y qué medidas deben tomar (no abrir enlaces sospechosos, cambiar contraseñas, desconfiar de llamadas o correos que usen datos médicos).

- **Responsable de ciberseguridad:** coordinar campañas internas de concienciación tras un incidente, reforzar los filtros de correo electrónico y aplicar reglas que detecten intentos de phishing basados en la información robada. El responsable debe asegurarse de que los pacientes y empleados estén prevenidos ante fraudes derivados de los datos robados.

- **Por qué funciona**: cuando los pacientes y el personal están preparados, la efectividad de los fraudes posteriores disminuye drásticamente, reduciendo el valor económico de los datos para los atacantes.

4. Cómo responder si el atacante publica los datos como represalia

- **Qué hacer en la clínica**: ten un protocolo de crisis reputacional que incluya comunicación con pacientes, medios y autoridades sanitarias. Reconoce el incidente, informa de las medidas de protección activas y explica los pasos que se están dando para prevenir que vuelva a ocurrir.

- **Responsable de ciberseguridad:** coordinar la recopilación de pruebas de la publicación, trabajar con las autoridades para solicitar la retirada de los datos en foros y reforzar los sistemas afectados para evitar nuevos accesos.

- **Por qué funciona:** aunque no siempre se puede evitar la publicación, sí se puede controlar el daño reputacional y demostrar que tu clínica actúa con responsabilidad y seriedad frente a la crisis.

Al aplicar las medidas de la Fase 7, esto es lo que consigues

Si tu clínica llega a esta fase con un plan de respuesta bien definido, el atacante podrá intentar extorsionar, vender o filtrar datos, pero su poder se reduce al mínimo. Tus copias de seguridad aisladas te permiten seguir funcionando, tu personal sabe cómo actuar ante fraudes derivados y tus pacientes confían porque reciben información clara y a tiempo.

En este escenario, el atacante pierde la mayor parte de su ventaja: sin capacidad de presión ni beneficio económico, lo más probable es que abandone y busque un objetivo más débil. En otras palabras: el ciclo del ataque puede acabar aquí, pero no necesariamente en tu contra.

Conclusión:

En España, además, sabes exactamente a quién recurrir: INCIBE-CERT, Policía Nacional o Guardia Civil, y la AEPD si hay datos personales comprometidos, tal y como marca el RGPD. Y recuerda que existen también marcos como NIS2, que refuerzan las obligaciones de ciberseguridad en el sector salud.

Lo más importante: todas estas tareas no pueden recaer en un dueño, un coordinador o una recepcionista sin formación técnica. Contar con un responsable de ciberseguridad, aunque sea externo, ya no es opcional. Es tan esencial como tener una higienista, una recepcionista o un doctor en tu clínica. Sin esa figura, todo lo que has leído en este manual esencial se queda en papel mojado.

Si alguna de las fases te ha generado dudas o quieres aclarar cómo aplicarlas en tu clínica, puedes escribirme y estaré encantada de responderte y ayudarte a entenderlo mejor. Y si lo que buscas es dar el siguiente paso, puedo crear para tu clínica un curso de ciberseguridad totalmente personalizado, adaptado a tu equipo y a vuestra forma de trabajar.

Mi experiencia en el sector salud y en ciberseguridad me permite diseñar formaciones prácticas, claras y efectivas. Ponte en contacto conmigo y empecemos a proteger tu clínica también en el mundo digital.

¿Quieres ver cómo piensa un atacante antes de aplicar estas medidas?
Descubre el artículo completo aquí:
Escanea el QR o visita: