AFAMEP
ASOCIACIÓN DE FACTURADORES MÉDICOS

GUÍA PRÁCTICA · 2026 – 2027

Herramientas Tecnológicas para el Facturador Médico

Cumplimiento HIPAA – HITECH, paso a paso

"La solución está accesible y, en algunos casos, gratuita."

José E. Delgado Torres, PMB-AI
Profesor AFAMEP
jedelgadotorres@gmail.com

Por qué esto te toca a ti, ahora

EL RIESGO ES REAL Y CRECIENTE

2026
319

2025
772

brechas grandes

Reportadas a la Oficina de Derechos Civiles (OCR). Principal razón: Hackinh, Ransomware y filtración de servidores en la nube.

≈140M

personas afectadas

por esas brechas en un solo año.

2013

último cambio mayor

la Regla de Seguridad no se moderniza desde entonces.

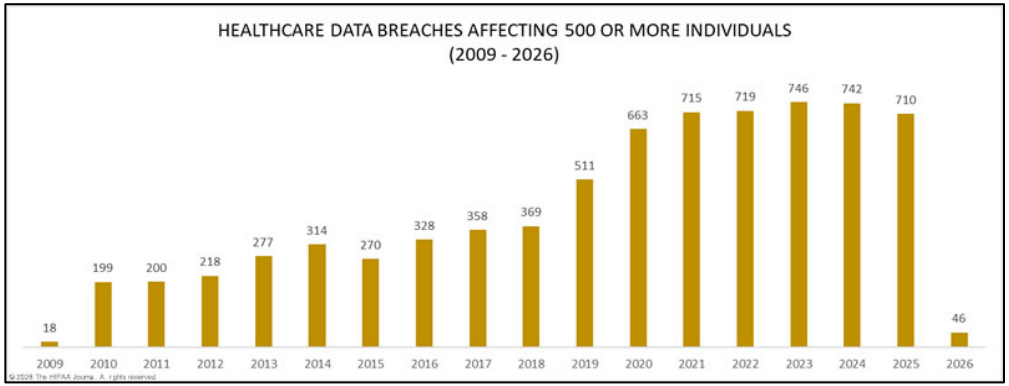
La OCR ahora sanciona a los **socios comerciales** igual que a los proveedores.

Un facturador médico crea, recibe y transmite información de salud protegida electrónica (ePHI). Eso te convierte en socio comercial (Business Associate) y te hace directamente responsable ante la ley — no solo ante tu cliente.

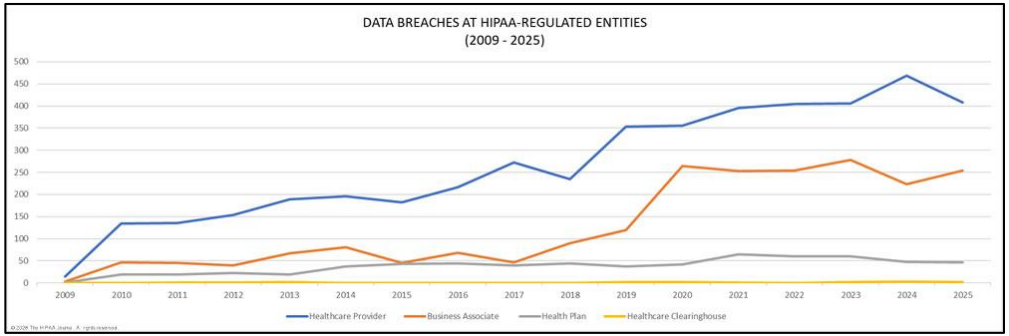
¿Por qué la urgencia de este cambio?

ALTO NIVEL DE ATAQUES AL CAMPO DE LA SALUD

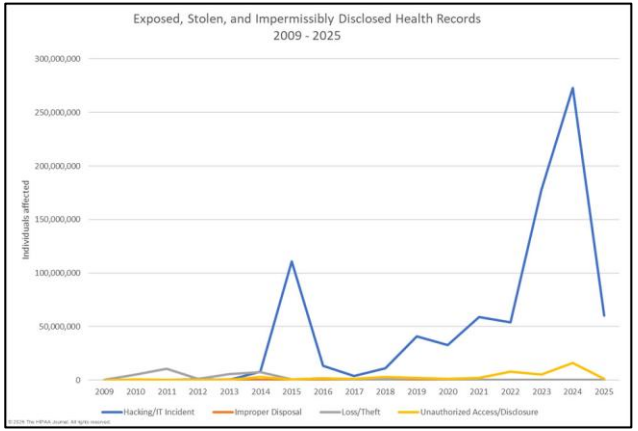
Fuga de datos afectando más de 500 personas



Fuga de datos de proveedores, socios de negocio, aseguradoras, clearinghouses



Casos de fuga por data expuesta, robada o revelada del EMR/EHR.



The HIPAA Journal
Healthcare Data Breach Statistics
– Updated for 2026

HIPAA y HITECH

LO MÍNIMO QUE DEBES DOMINAR

Regla de Privacidad	Qué información puedes usar y divulgar, y los derechos del paciente sobre ella.
Regla de Seguridad	Salvaguardas administrativas, físicas y técnicas para proteger la ePHI.
Notificación de Brechas	A quién avisar, cómo y en cuánto tiempo cuando la información se expone.
Ley HITECH (2009)	Extiende la responsabilidad directa y las sanciones a los socios comerciales.

Regla práctica: si tocas ePHI, las cuatro te aplican — sin importar el tamaño de tu operación.

Qué cambia entre 2026 y 2027

CALENDARIO REGULATORIO

Enero 2025
Propuesta publicada

La OCR publica el reglamento propuesto (NPRM) para modernizar la Regla de Seguridad.

Marzo 2025
Cierre de comentarios

Más de 4,000 comentarios de la industria sobre costo y plazos.

16 de febrero 2026
Ventana de preparación

La regla vigente sigue en efecto. Es el momento de implementar sin presión.

Julio 2027
Regla final proyectada

El proyecto RIN 0945-AA22 se pasó a la lista de “Acciones a largo plazo” por la complejidad regulatoria se retrasó el proyecto.

La prórroga no es una pausa… es tu ventaja

La fecha final se movió de **mayo de 2026** a **julio de 2027**, pero casi todo lo propuesto ya es buena práctica exigible hoy bajo el análisis de riesgo. Implementarlo ahora cuesta menos que hacerlo contra reloj.

Regla de Seguridad de HIPAA

SEGURIDAD CIBERNETICA

Nueva fecha proyectada: Julio 2027

Más de 100 organizaciones de salud en E.U. (CHIME, organización de Chief Information Officers) exigieron retirar o mitigar la propuesta por los altos costos de cumplimiento.

Análisis de Riesgo

Realizar evaluaciones de riesgo mucho más detalladas y complejas con más frecuencia.

Escaneo de vulnerabilidad

Cada 6 meses ejecutar escaneos técnicos de vulnerabilidad de forma estricta.

Inventario y mapas de red

Revisar anualmente un inventario de activos tecnológicos y mapas de redes.

Eliminación de flexibilidades

Se vuelve obligatorio todos los estándares técnicos sin importar el tamaño del proveedor.

Autenticación Multifactor (MFA)

Implementación obligatoria de MFA en todos los accesos aplicables.

Capacitación de personal

Se requiere inversion substancial y tiempo para entrenar al personal a las nuevas reglas.

¡Todo se vuelve obligatorio!

Regla de Privacidad de HIPAA

AGOSTO DE 2026

Revisar e implementar los siguientes puntos

Para alinearte al nuevo panorama regulatorio.

1 Reducción de tiempo al acceso de data PHI

Entrega del historial medico a un paciente a un mínimo de 15 días las instituciones y 5 días las oficinas médicas. Si el paciente tiene alguna deuda, deducibles o consulta la ley prohibe a la oficina a usar eso como mecanismo de presión para cobro. Se puede cobrar a .75¢ por página a un máximo de $25.00 por todo el record.

Carta de derecho y responsabilidad del paciente.

Ley 309-2002

2 Inspección en persona y derecho a revisión/cambio

Hay que entrenar personal para designar un área Segura y privada para que el paciente pueda verificar, arreglar y tomar notas de su data PHI almacenada en el récord.

3 Actualización del Aviso de Prácticas de Privacidad (NPP)

Asegurar que el documento de aviso tenga integrado las reglas de confidencialidad de registro de adicciones y trastornos por el uso de sustancias. También tiene que tener transparencia de costos.

Regla de Privacidad de HIPAA

AGOSTO DE 2026

Revisar e implementar los siguientes puntos

Para alinearte al nuevo panorama regulatorio.

4

Acceso digital a su información del récord

La práctica médica debe contar con un protocol técnico y administrativo para enviar la data PHI electrónicamente encriptada o acceder a su data del EMR/EHR del doctor a solicitud del paciente si lo pide formalmente.

5

Nuevas plantillas de divulgación y políticas

Revisar sus políticar internas de divulgación ante emergencias. El estándar amplía para permitir divulger PHI con el fin de evitar amenazas a la salud o seguridad cuando el daño sea “seria y razonablemente previsible” (antes se requería ser inminente). Inclusive la protección y la prohibición absoluta de divulgar información con cuidados de salud reproductiva.

Regla de Privacidad de HIPAA

CONTEXTO DE FACTURADOR

AGOSTO DE 2026

Revisar e implementar los siguientes puntos

Para alinearte al nuevo panorama regulatorio.

1 El estándar del “Mínimo Necesario”

Se debe implementar controles de acceso basado en roles en tu software de facturación. El personal de facturación solo debe visualizar lo mínimo y lo esencial para poder trabajar una factura nunca el historial clínico completo o evolución si no es estrictamente necesario para resolver alguna situación de denegación.

2 Bloqueo de exportación masiva de datos

Debes tener control y auditar todas las exportaciones masivas de datos a menos que sean pedidos de auditorías externas. En tu Sistema debes identificar usuarios accesando y descargando información masiva de datos.

3 “Blindaje” del trabajo remoto (Seguridad ePHI)

El trabajo remoto del facturador independiente es común, para este period de cumplimiento, queda estrictamente prohibido que accedas a portales e información sensible desde redes Wi-Fi públicas/gratis y/o computadoras sin medidas de protección implementadas. Debes garantizar el uso de VPN, autenticación multifactor (MFA) obligatoria para iniciar session en los sistemas de facturación y el bloqueo automático de pantallas tras periodos de inactividad.

Lo que la propuesta te va a exigir

OCHO CAMBIOS DE FONDO

1. **Adiós a lo “opcional”**
   Casi todas las salvaguardas pasan a ser obligatorias.

2. **Autenticación multifactor**
   MFA obligatoria en todo acceso a sistemas con ePHI.

3. **Cifrado en reposo y en tránsito**
   Ya no queda a tu criterio: se exige por defecto.

4. **Inventario y mapa de red**
   Lista de activos y flujos de ePHI, revisada cada año.

5. **Análisis de riesgo escrito**
   Documentado, con metodología y actualizado anualmente.

6. **Pruebas técnicas periódicas**
   Escaneo de vulnerabilidades y pruebas de penetración.

7. **Recuperación en 72 horas**
   Plan probado para restaurar sistemas críticos.

8. **Verificación de proveedores**
   Confirmar por escrito y cada año las salvaguardas de tus socios.

Tu posición legal… eres socio comercial

BUSINESS ASSOCIATE

Manejas ePHI para un tercero

Códigos, reclamaciones, elegibilidad, expedientes.
Todo eso es información de salud protegida.

Cuatro obligaciones que no puedes delegar

1. Firmar un acuerdo de socio comercial (BAA) con cada proveedor médico que atiendes.
2. Firmar BAAs con tus propios subcontratistas que tocan ePHI.
3. Cumplir la Regla de Seguridad por cuenta propia, no “bajo el paraguas” del cliente.
4. Notificar brechas a tu cliente sin demora irrazonable.

Sin un BAA firmado, cada intercambio con tu cliente ya es una violación — antes de cualquier ataque.

EL RIESGO

Thumbcache.db

Temporary Files

Copilot+ / Windows Recall

El archivo que recuerda lo que ya borraste.

Riesgo del Thumbcache.db

CONTEXTO DE FACTURADOR

RIESGO EN 45 CFR 164

1 Violación del criterio de "Información no cifrada"
(Breach Notification Rule)

RIESGO	HIPAA exige cifrar el ePHI tanto en tránsito como en reposo. Aunque el archivo sea eliminado de la computadora el Thumbcache.db guarda una copia legible en el disco duro de forma permanente.
HITECH	Si la computadora es robada, hackeada o vendida sin una limpieza forense, las miniaturas del Thumbcache.db se consideran datos expuestos no cifrados. Esto es considerado un Data Breach.

2 Incumplimiento de las Reglas de Destrucción de Datos
(Media Sanitization – 45 CFR 164.310(d)(2))

RIESGO	Si un facturador elimina el archive de su computadora y vacía el "Recycle Bin" assume que cumplió con la eliminación. Sin embargo, un auditor forense puede extraer el archive y reconstruir visualmente los documentos eliminados. Terceros pueden utilizar herramientas (gratis) para visualizar la foto.

Riesgo del Thumbcache.db

CONTEXTO DE FACTURADOR

RIESGO EN 45 CFR 164

3 Severidad en Penalidades Financieras

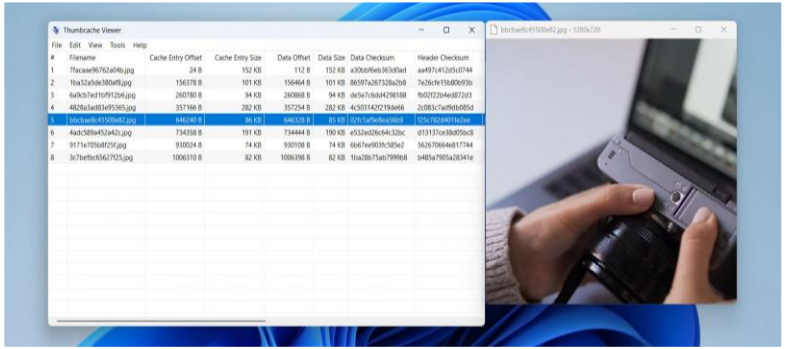
RIESGO

La ley HITECH endureció dramáticamente las multas por violaciones de HIPAA. Si se descubre que un facturador ha estado acumulando ePHI de manera negligente a través del cache de Windows debido a una falta de supervisión o la ausencia de políticas de IT correctas, la organización se enfrenta a multas que escalan rápidamente según el nivel de culpabilidad:

- **Falta de supervision (Lack of Oversight)** • desde $1,424 por violación (por cada imagen de Thumbcache).
- **Negligencia deliberada (Willful Neglect)** • hasta $2 Millones annual si el problema no se corrige.

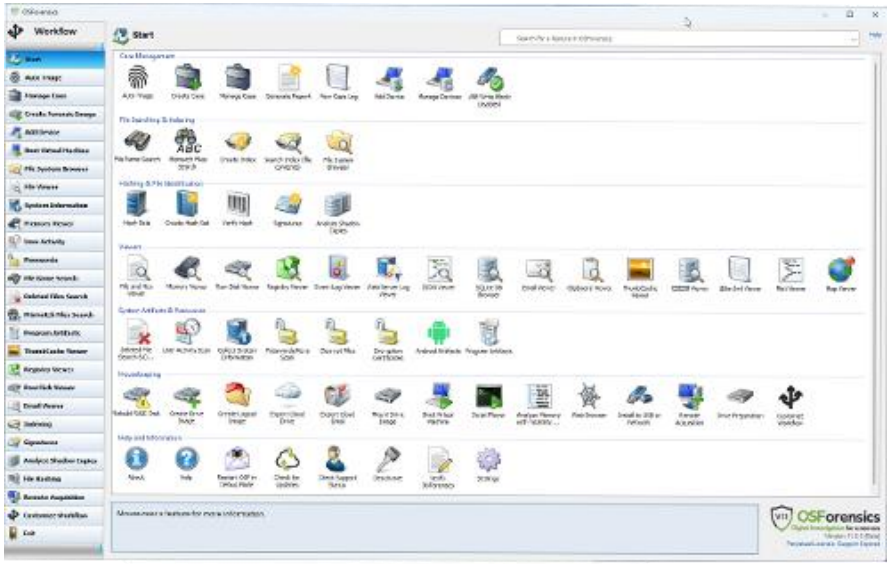
¿Cómo visualizar las imagenes Thumbcache.db?

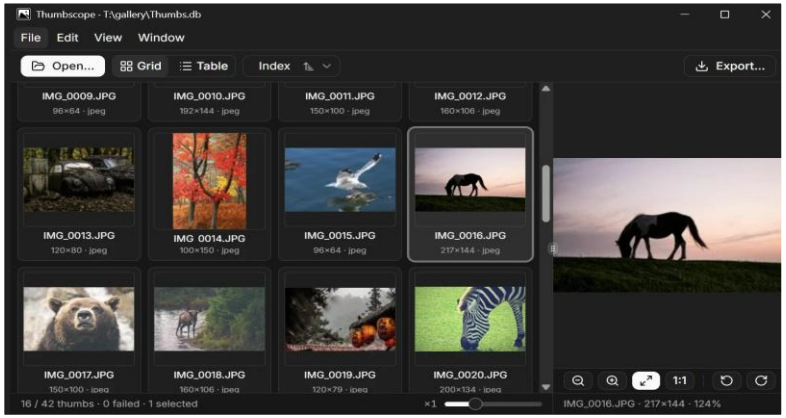
Thumbcache Viewer *(gratis)*



OSForensics

$945 anual – *(tiene acceso a un Free Trial)*





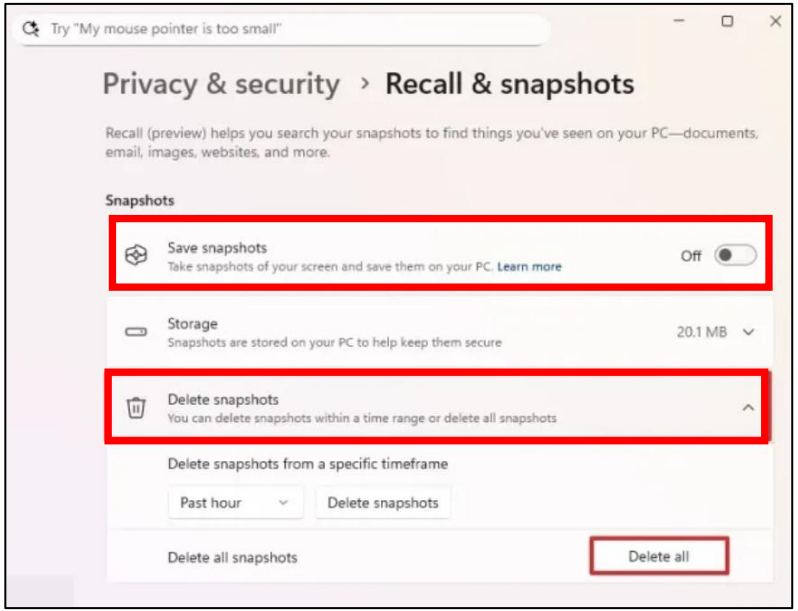
Thumbscope *(gratis)*

Windows Recall

MEMORIA VISUAL DEL SISTEMA

1. **Función de IA en PC Copilot+ con Windows 11: toma fotos instantáneas de la pantalla aproximadamente cada cinco segundos cuando el contenido cambia.**
2. **Las fotos instantáneas se guardan localmente y se indexan para búsquedas en lenguaje natural.**
3. **En una pantalla de facturación, eso significa nombres, diagnósticos, números de póliza y códigos capturados sin intención.**
4. **El filtro de "información sensible" es incompleto: pruebas independientes han mostrado que deja pasar datos como números de cuenta y de seguro social.**
5. **Una función que copia ePHI a un almacén local no declarado no cabe en un análisis de riesgo sin controlarla.**

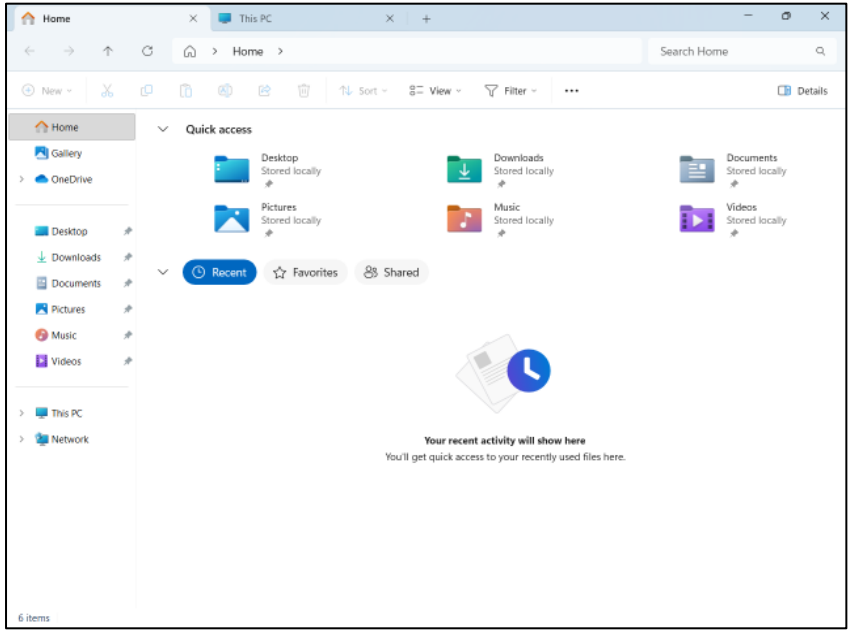
¿Cómo desactivar Windows Recall?



1. Abres Settings
2. Presiona en el menu de la izquierda “Privacy & Security”
3. Selecciona “Recall & Snapshots”
   - Save snapshot – Off
   - Delete snapshot – Delete all
4. Confirmar

Windows ya avisó que esta opción se reactiva cada cierto tiempo y en cada actualización del Sistema, ¡debes estar pendiente a esto!.

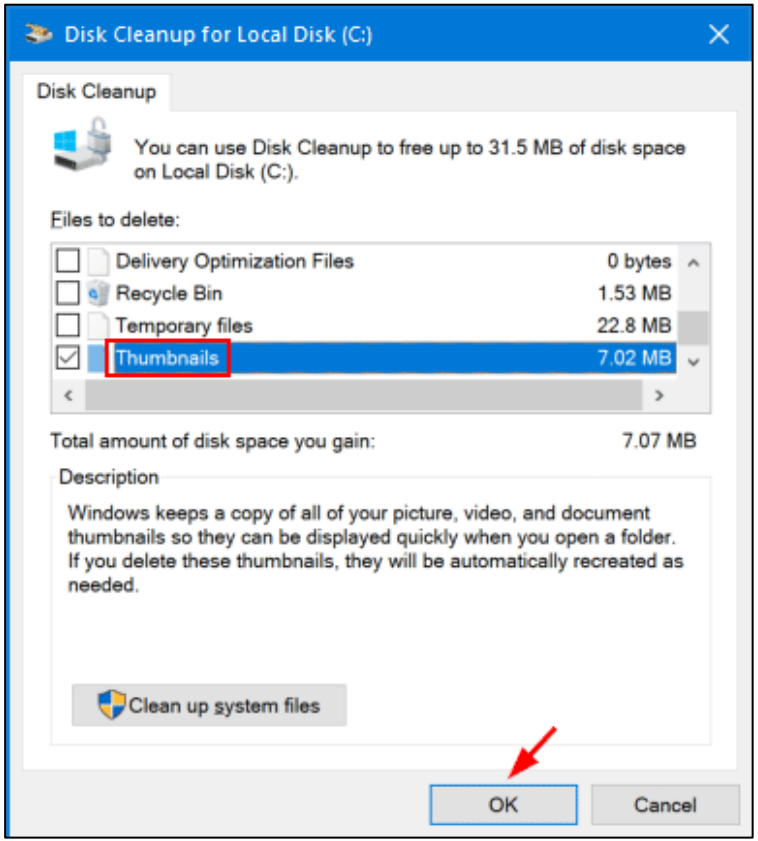
¿Cómo desactivar Thumbcache.db?



1. Abres el File Explorer (Windows key + E)
2. Presionas el tab de View
3. En Folder Options presionas View Tab
4. En ”Advance Settings” escoges “Always show icons, never thumbnails”
5. Presionas Apply
6. Presionas OK

Esta es la major manera de hacer “Media Sanitization”.

¿Cómo borrar el Thumbcache.db?



Windows tiene una aplicación interna llamada **Disk Cleanup**.

1. Buscar y abrir **Disk Cleanup**
2. Seleccionas el Drive (Local Disk C)
3. Seleccionas **Thumbnails** y hasta los **Temporary Files**
4. Presionas **OK** para ejecutar la selección de borrar

Esto elimina al momento todo lo almacenado. Liberas espacio de computadora y mejora el performance del equipo. Si solo borras y no desactivas Thumbcache el próximo file que abras se crea otra imagen y comienza el ciclo.

Siempre que se haga una actualización del Sistema se debe verificar si está activo, de estarlo Volver a hacer los pasos para borrar todo.

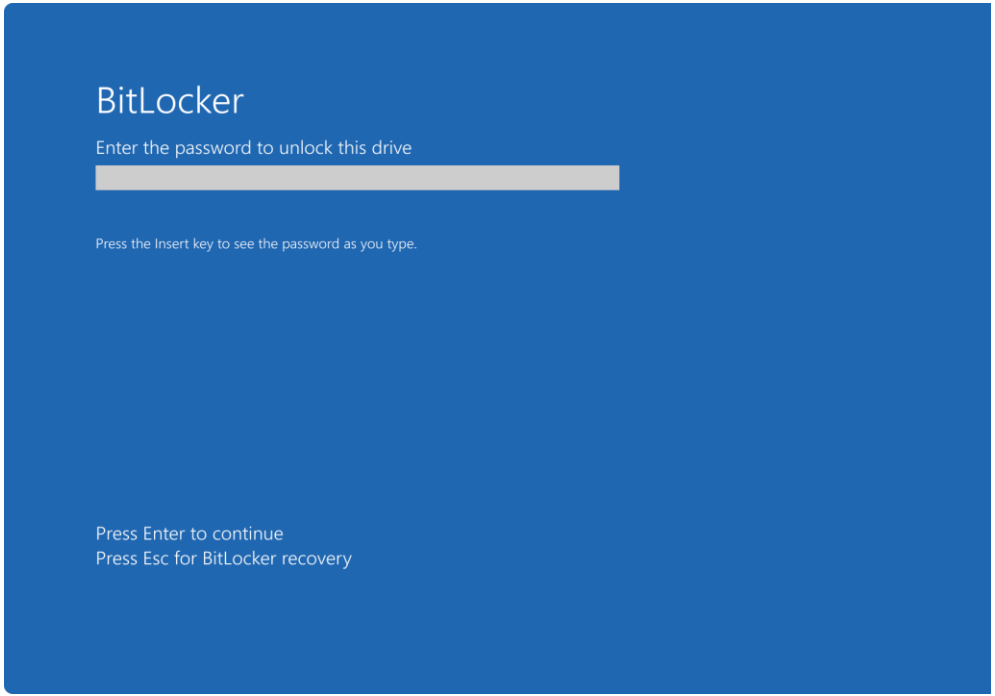
SALVAGUARDAS TÉCNICAS

HERRAMIENTAS DISPONIBLES

GRATIS...
CASI GRATIS...
Y LO QUE SI SE PAGA.

Cifrado de computadora

GRATIS



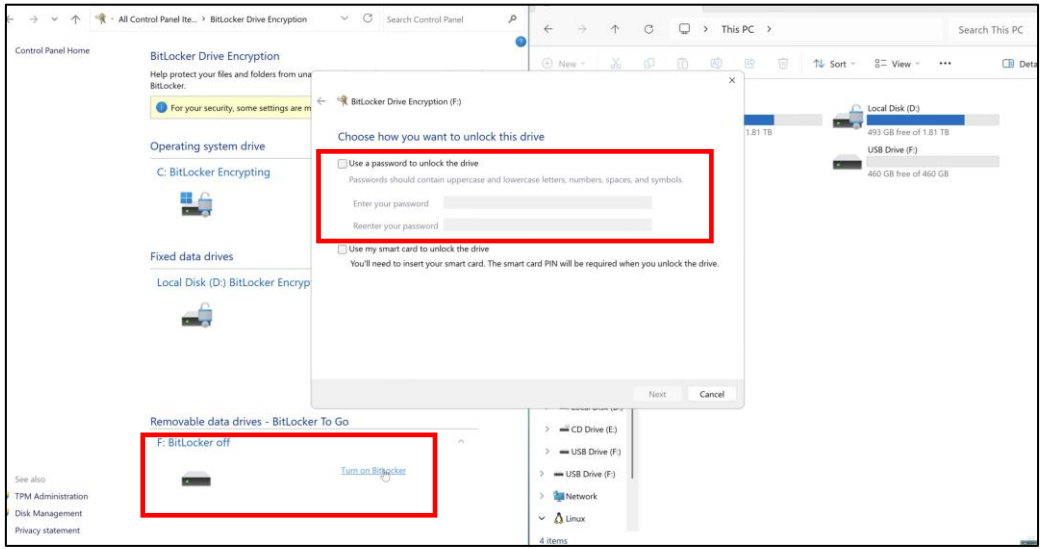
- **Control Panel**
- **System and Security**
- **BitLocker Drive Encryption**

Pueden hacer un search en la computadora a BitLocker

Aseguren salvar el Recovery Key de 48 dígitos que se provee por si olvidas tu password de BitLocker.

Cifrado de USB / Hard Drive Externo

GRATIS



1. Conectas el USB / Hard Drive Externo
2. Presionas Windows + E escoges “This PC”
3. En el USB escoge “Turn on Bitlocker”
4. Escribe el password y lo confirmas

Otras cosas que puede pedir sea las opciones de cifrado:

- **Encrypt used disk space only:** Para un USB totalmente nuevo y vacío y lo encriptas por primera vez.
- **Encript entire drive:** Para un USB que ya tiene uso y no es nuevo.

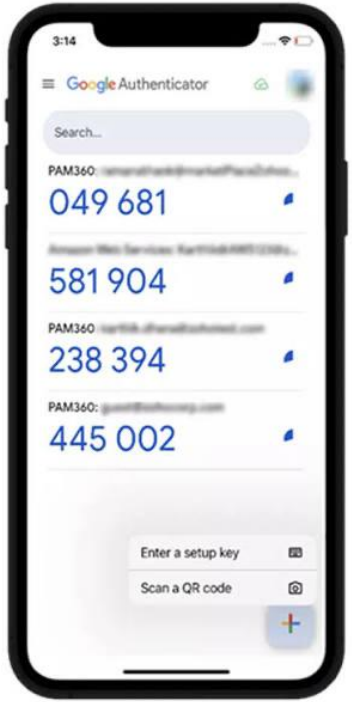
Cada vez que conectes el USB o Hard Drive Externo a una computadora te va a pedir password.

Esto es algo que debe ser implementado obligatoriamente desde ya.

Multi-Factor Authenticator

GRATIS / PAGANDO

Mobile APP - GRATIS



okta

Duo Mobile

Google Authenticator

Tokens (1 time payment)

$30.00

YubiKey *5C NFC*

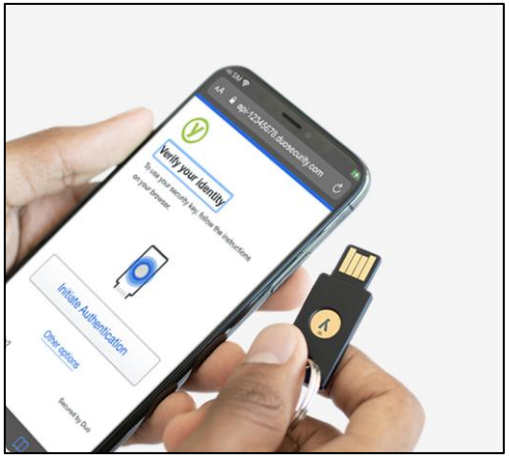
$30.00 a $98.00

5C: Conector USB-C android, ipad/iphone, Macbook, PC Laptop.

NFC: Huella digital como password o un simple plug en el dispositivo y se activa el proceso de autenticación.

Multi-Factor Authenticator

PAGANDO



Protección básica de Phishing o accesos a cuentas sin necesitar password una vez activado.

YubiKey *NFC*

$30.00

YubiKey 5C
YubiKey 5 NFC

$58.00

YubiKey Bio

$98.00

Administradores de contraseñas

PAGANDO

KEEPER Cybersecurity Starts Here™

$1.80 a $7.00 al mes

1Password

$2.99 a $4.50 al mes

bitwarden

$4.00 a $6.00 al mes

La aplicación es un plug-in del browser, solo necesitas recordar un password principal y la aplicación se encarga de completar los campos user/password y puede ayudar a crear passwords seguros.

Características Clave Requeridas

- **Cifrado "Zero Knowledge"** solo el usuario tiene acceso a su base de datos de passwords.
- **Multifactor Authentication** Capa adicional de validación de acceso.
- **Control administrativo y auditoria de accesos** Capacidad de auditora inicios de sesión y revocación de permisos centralizado.

Cifrar archivos ZIP

GRATIS / PAGANDO

Archivo digital

- **Cifrado (Encriptar)**
- **Copias de seguridad**
- **Disposición final** *(después de los 10 años)*

GRATIS:

7zip

WinRAR

VeraCrypt

^ Implementen usar esta preferiblemente.

AxCrypt ***$45.00 anual***

Los archivos Zip se pueden reconocer de estas 2 manera.

WINDOWS

MacOS

La nueva regla exige que los archivos que no esten utilizandose deben estar encriptados.

Cyber Liability Insurance

PAGANDO

First Party Coverage

Cubierta para costear recuperación, restauración y reparación de data, reembolso por perdida de ingreso debido a interrupción del negocio y extorsión (Ransomware).

Third Party Coverage

Cubierta de defensa legal, reclamaciones de privacidad del cliente y multas regulatorias.

Manejo de Crisis

Cubierta para fondos de invertigación forence, relaciones públicas y negociaciones con clientes afectados.

Póliza básica de Oficina

Cobertura de $1,000,000

$1,200 a $2,400 ANUAL

Póliza básica de Independiente

Cobertura de menos de $1,000,000

$360 a $720 ANUAL

**Precios pueden variar según region donde estas, póliza, tamaño de la empresa u oficina médica, cubierta y auditoria de la aseguradora.*

GEICO CHUBB mapfre Multinational

Para calificar a estos seguros tus procesos tienen que estar en cumplimiento de la HIPAA, tienes que tener equipo encriptado, MFA y métodos básicos de ciberseguridad en la oficina.

Inventario de Activos

GRATIS / PAGANDO

Template creado y aprobado por HHS y la Oficina de Derechos Civiles

Tiene documentos de Excel que pueden descargar y completar los campos requeridos

https://healthit.gov/privacy-security/security-risk-assessment-tool/

Template de IT Asset Inventory Tracker

Es un documento con el formato NIST SP 800 (HIPAA Compliant)

https://www.nanosoftltd.com/resources/it-asset-inventory-tracker-free-excel-download

Protección de Endpoint Detection and Response (EDR)

PAGANDO / CASI GRATIS

¿Cómo funcionan?

Colección de data que está pendiente a cambios en archivos, conecciones y Comunicaciones entre procesos. Normalmente viene con un AI integrado que aprende de como te comportas y como usas la computadora y si te desvías tira un alerta de actividad maliciosa. Tiene un panel de análisis de todo lo que ocurre en la computadora y hace un timeline de cuando comenzó el ataque y que se hizo.

SOPHOS

$50.00 a 60.00 al año por licencia

Microsoft Defender

Incluido gratis con Windows 10/11

Para incluirlo a más de 1 dispositivo se require licencia Microsoft365 Desde $70.00 al año.

Herramientas extras

GRATIS

https://www.virustotal.com

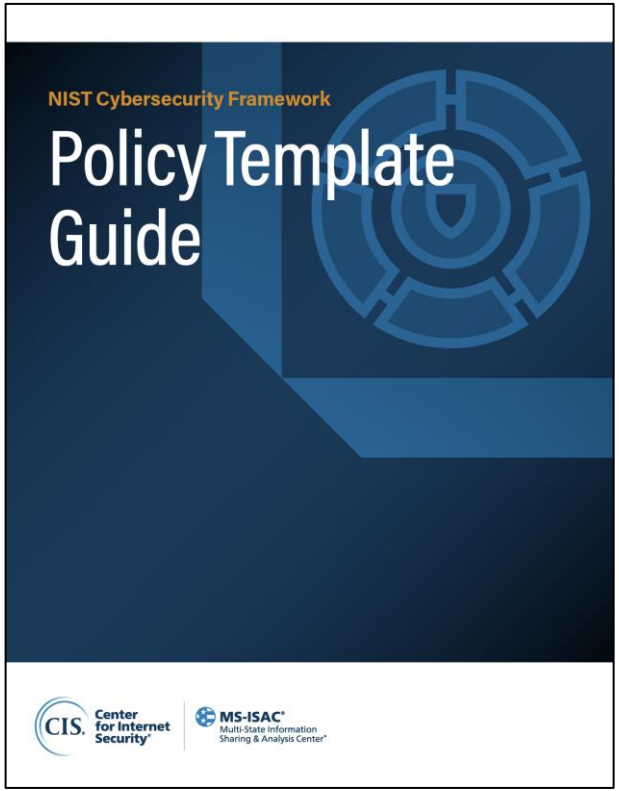
No estas segura/o que el documento, dirección URL que te compartieron es seguro...

Puedes filtrarlo por este website.

Este website filtra los documentos y URL por 75 softwares y páginas de verificación y te dice si tiene algún virus o algún software malicioso y de tenerlo te dice cual virus, worm, malware, spyware.

Herramientas extras

GRATIS



NIST Cybersecurity Framework (Template)

(National Institute of Standards and Technology)

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NIST es una agencia *(no federal)* **del Depto. de Comercio de E.U. que creó y mantiene las guías y marcos de referencia a nivel global de como se mide y desarrolla los estándares de calidad en la gestion de manejo de riesgos y ciberseguridad.**

No lo dejes con el texto genérico que tiene, actualizen los Placeholder a nombre de tu persona, LLC, compañía con los parametros que le corresponde a ustedes.

El documento tiene links donde baja el formato en un WORD.

NIST Cybersecurity Framework (Template)

(National Institute of Standards and Technology)

Mapa de inventario de su sistema: Antes de comenzar todo haga una lista de todos los equipos que se utilizan en su trabajo, softwares y softwares de facturación si es cloud, server, si utiliza herramientas Third Party incluyendo Inteligencia Artificial.

Realiza un analisis de brechas: Compare sus prácticas operativas actuales, si el NIST te pide hacer una revisión semanal pero usted nunca los revisa, marque como una ”acción crítica pendiente”.

Convierte las reglas en procedimientos: La regla indica a empleados que hacer, mientras que el procedimiento les explica como hacerlo. Una de las políticas debe ser cada periodo de tiempo se debe hacer un backup fuera de horas pico de toda la información. Puedes tener un ”Cloud Storage” aislado de la información de tu trabajo.

Capacitación personal y de sus empleados: Uno mismo y los empleados son la entrada mas frecuente de los ataques de Phishing. Capacite para hacer sesiones formativas breves y obligatorias sobre cómo identificar correos electrónicos falsos.

NIST Cybersecurity Framework (Template)

(National Institute of Standards and Technology)

Estructure sus políticas

Asset Management & Access Control Policy: Establece quién tiene acceso a sus cuentas de Clearinghouse y los softwares que utiliza para facturación (incluye nombre de softwares).

Política de protección de datos: Define como se manejan, almacenan y cifran los datos.

Política de respuesta ante incidents y recuperación: Establece procedimientos paso a paso para actuar en caso de que un ataque de Ransomware todos sus archivos tienen que estar cifrados.

https://www.nist.gov/cyberframework/csf-20-quick-start-guide-template-options

Opción 1: Una guia de como utilizar el NIST en un pequeño negocio.

Opción 2: Una guia de como implementar ciberseguridad paso a paso en su oficina.

Hábitos diarios del facturador que evitan una brecha

CONDUCTA EN LA ESTACIÓN DE TRABAJO

1. **Bloquear la pantalla siempre al levantarse, aunque sea por unos minutos.**
2. **Filtro de privacidad si el monitor se ve desde fuera de la oficina o front desk del consultorio.**
3. **Nada de capturas de pantalla de récords ni fotos con el celular personal.**
4. **No guardar ni dejar visible PHI/ePHI en el área de trabajo.**
5. **Vaciar el “Recycle Bin” y los archivos temporales (Temp files) al acabar jornada.**
6. **Prohibido usar el equipo de trabajo para uso personal.**
7. **Reportar de inmediato cualquier pérdida, robo o comportamiento raro del equipo.**

Cuánto cuesta realmente cumplir

GRATIS, CASI GRATIS Y LO QUE SÍ SE PAGA

Gratis

- Security Risk Assessment (SRA) Tool del HHS
- Cifrado BitLocker (PC) / FileVault (Apple)
- Autenticación multifactor (MFA)
- Protección integrada del sistema
- Materiales de capacitación

Bajo costo

- Correo con BAA (~$6–15/usuario)
- Respaldo en nube (~$5–20/mes)
- Gestor de contraseñas de equipo
- VPN para trabajo remoto
- Simulacros de phishing

Inversión

- Escaneo de vulnerabilidades
- Prueba de penetración anual
- Asesoría legal para BAAs
- Equipo de reemplazo sin soporte

Una oficina de facturación de una (1) a tres (3) personas puede alcanzar un nivel sólido de cumplimiento por menos de $50 al mes, más el tiempo dedicado a documentar.

Tu plan de los próximos 90 días

¡EMPIEZA EL LUNES!

Esta guía es orientación general de cumplimiento, NO ES asesoría legal.

Días 1–30

- Inventario de activos y mapa del flujo de ePHI
- Análisis de riesgo con el SRA Tool
- Cifrado de ZIP en todos los archivos
- Cifrado de disco en todos los equipos
- Protección contra archivos maliciosos

Días 31–60

- MFA en todos los accesos que sea posible
- Correo electrónico (domain) cifrado
- Gestor de contraseñas y cuentas individuales

Días 61–90

- Respaldo probado y tiempo de restauración medido (Business Continuity) en una emergencia
- Capacitación documentada del personal
- Revisión de todos los BAAs

Los tres errores que más caro se pagan

1. No tener el análisis de riesgo por escrito y análisis de vulnerabilidad y penetración certificado.
2. Usar correo electrónico sin protección o servicio de almacenamiento cloud sin BAA firmado.
3. No tener un servicio de Business Continuity en un incidente de emergencia.


¡GRACIAS!