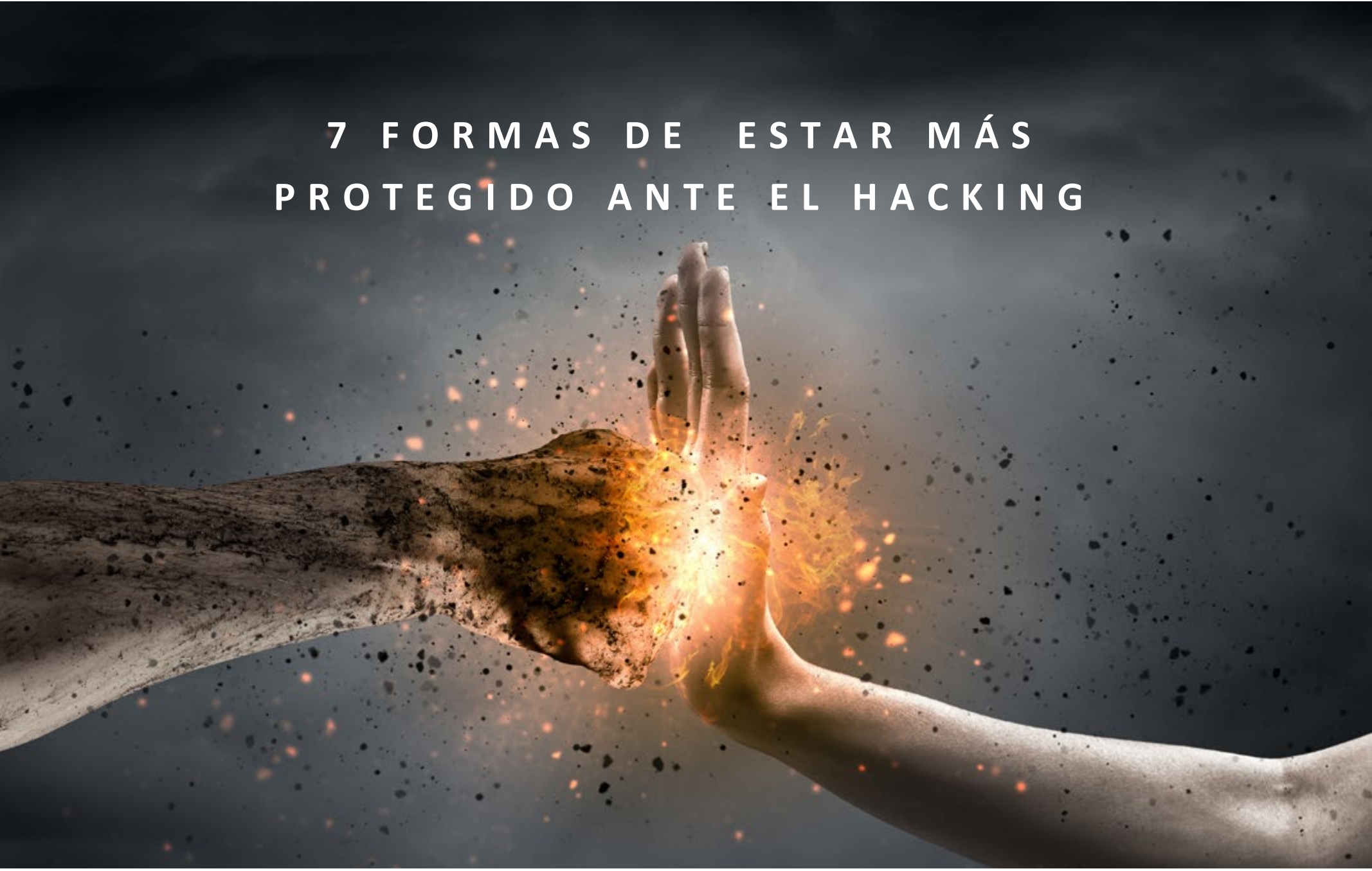
7 FORMAS DE ESTAR MÁS PROTEGIDO ANTE EL HACKING



OnTek

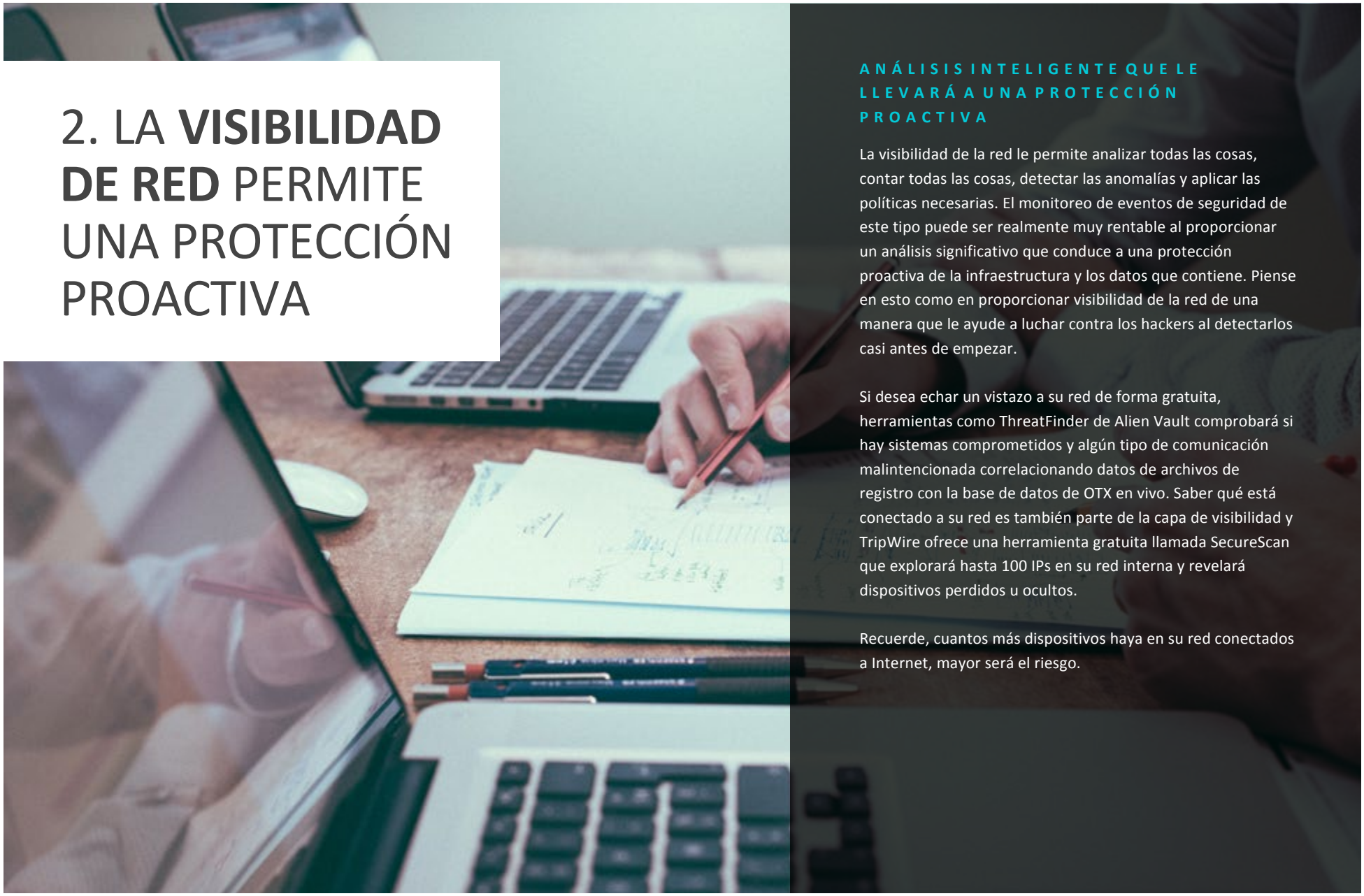
1. ADOPTE UN **ENFOQUE POR CAPAS** EN TEMAS DE SEGURIDAD

UN ENFOQUE QUE LE PROVEERÁ DEL TIEMPO QUE NECESITA

Llámele seguridad en capas o defensa en profundidad, pero sólo asegúrese de que lo está usando. Aunque el concepto es tan antiguo como el pensamiento de seguridad de TI en sí mismo, eso no quita que, aplicar capas de seguridad, sea menos relevante hoy en día. La elección de las capas correctas, por supuesto, es primordial. Piense en la defensa en profundidad como una estructura de mitigación de riesgos aplicando capas múltiples de control a lo largo y ancho de su entorno de TI.

Hacer esto no garantizará la prevención de ataques, pero los ralentizará y ayudará a proteger a su organización contra la inevitabilidad de esos ataques. Hecho correctamente, dará tiempo; El tiempo que necesita para responder efectivamente a cualquier ataque y aplacar una brecha potencial. En otras palabras, le hará más difícil de hackear.

Siga leyendo para descubrir las siete maneras de hacer que esto suceda.



2. LA **VISIBILIDAD DE RED** PERMITE UNA PROTECCIÓN PROACTIVA

ANÁLISIS INTELIGENTE QUE LE LLEVARÁ A UNA PROTECCIÓN PROACTIVA

La visibilidad de la red le permite analizar todas las cosas, contar todas las cosas, detectar las anomalías y aplicar las políticas necesarias. El monitoreo de eventos de seguridad de este tipo puede ser realmente muy rentable al proporcionar un análisis significativo que conduce a una protección proactiva de la infraestructura y los datos que contiene. Piense en esto como en proporcionar visibilidad de la red de una manera que le ayude a luchar contra los hackers al detectarlos casi antes de empezar.

Si desea echar un vistazo a su red de forma gratuita, herramientas como ThreatFinder de Alien Vault comprobará si hay sistemas comprometidos y algún tipo de comunicación malintencionada correlacionando datos de archivos de registro con la base de datos de OTX en vivo. Saber qué está conectado a su red es también parte de la capa de visibilidad y TripWire ofrece una herramienta gratuita llamada SecureScan que explorará hasta 100 IPs en su red interna y revelará dispositivos perdidos u ocultos.

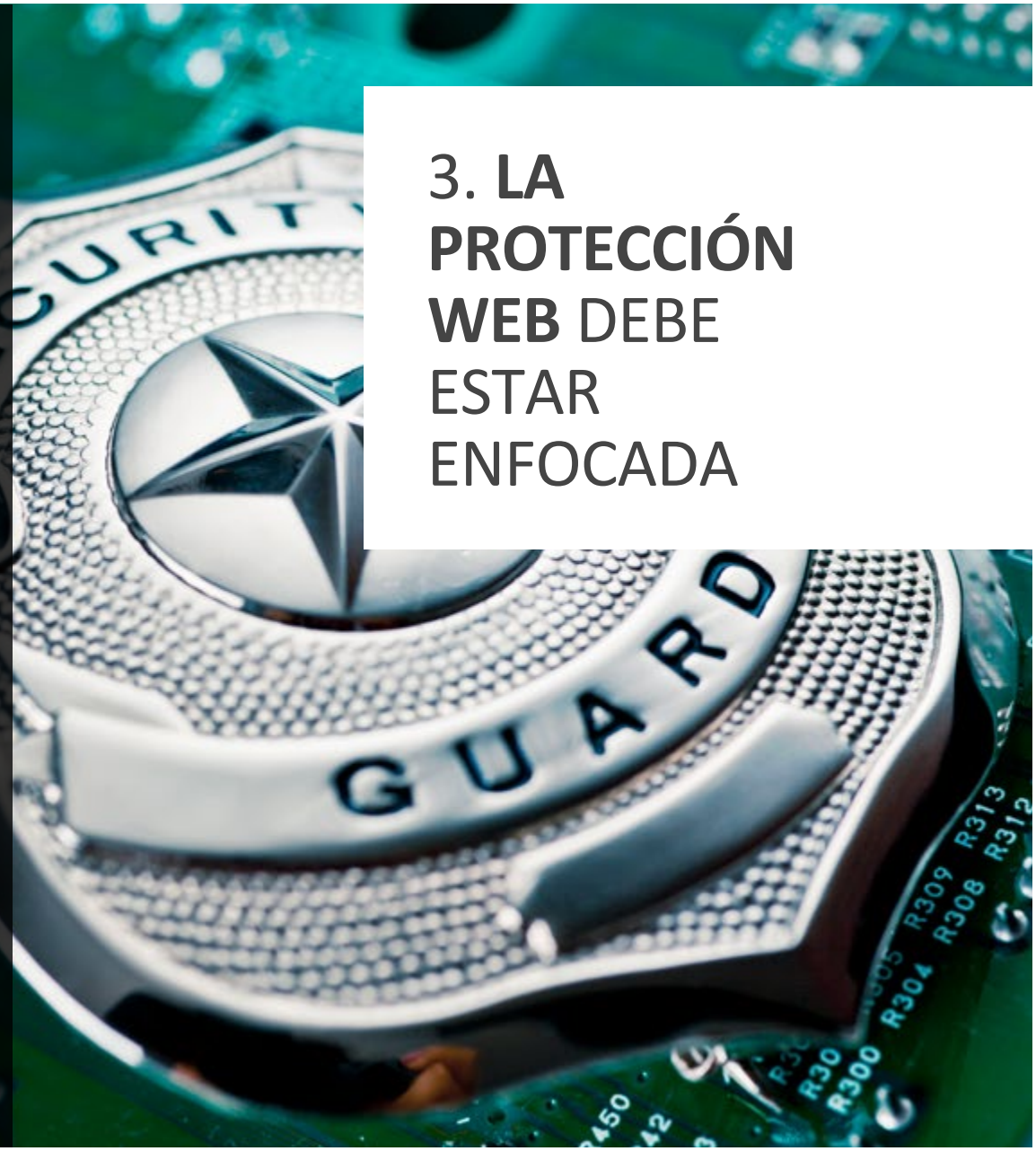
Recuerde, cuantos más dispositivos haya en su red conectados a Internet, mayor será el riesgo.

CONTROL, MONITORIZACIÓN Y REFUERZO DE LAS POLÍTICAS WEB

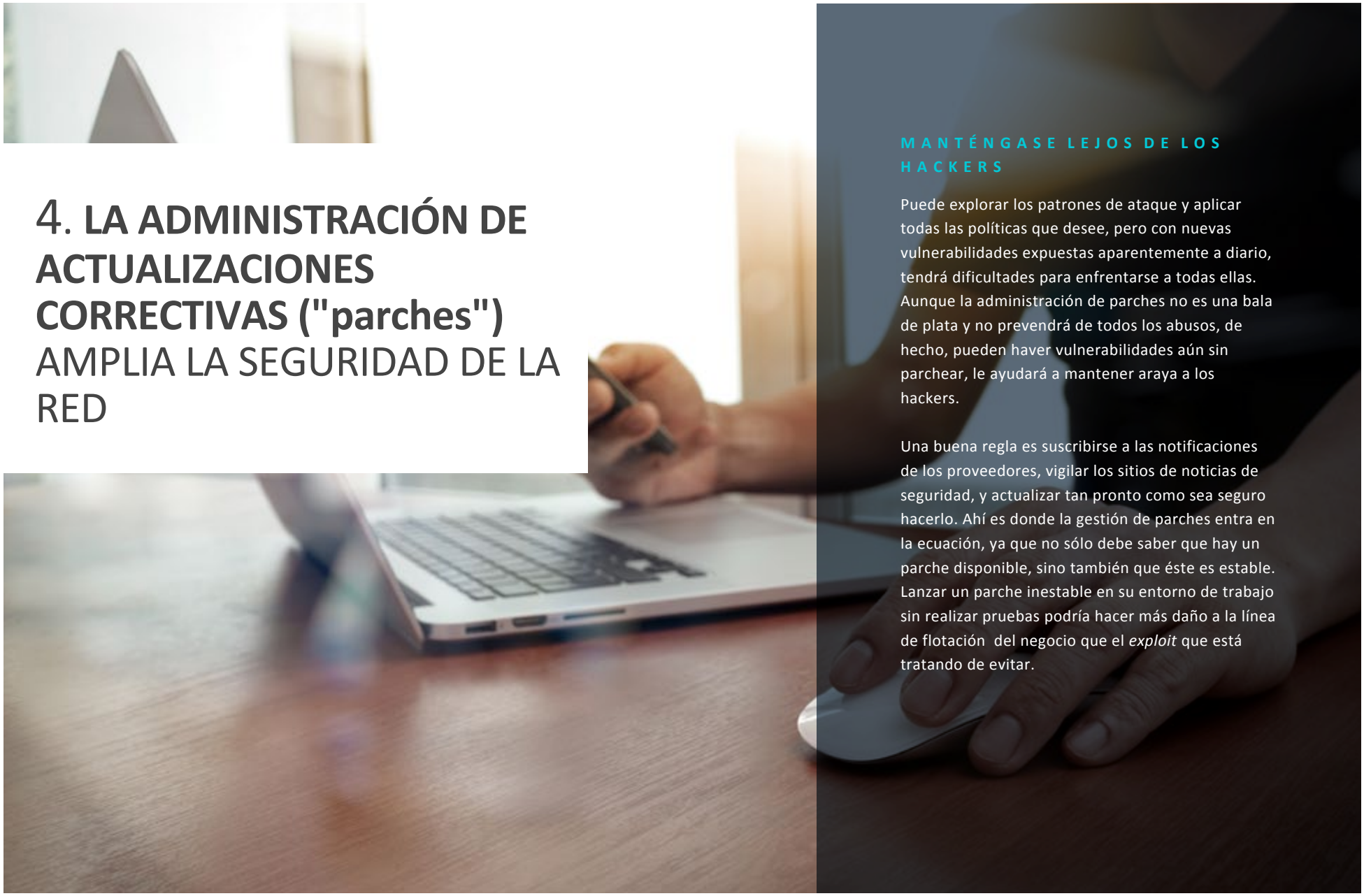
La protección web es otra capa esencial de seguridad, proporcionando una ventana para controlar, supervisar y hacer cumplir las políticas web de los clientes a través de un único front-end. De hecho, la mejor manera de pensar que la protección de la web es hacerlo como un enfoque de seguridad basado en políticas. Múltiples dispositivos pueden apuntar a una política central que puede ser editada y escalada para adaptarse a una serie de dispositivos de este tipo, en lugar de tener ajustes a nivel de dispositivos.

Hacer esto le permite aplicar el filtrado de sitios web por tiempo o contenido, realizar el control de ancho de banda para evitar el estrangulamiento de la red y, en última instancia, ayudar a proteger a la empresa contra la responsabilidad legal.

3. **LA PROTECCIÓN WEB** DEBE ESTAR ENFOCADA



4. **LA ADMINISTRACIÓN DE ACTUALIZACIONES CORRECTIVAS ("parches")** AMPLIA LA SEGURIDAD DE LA RED

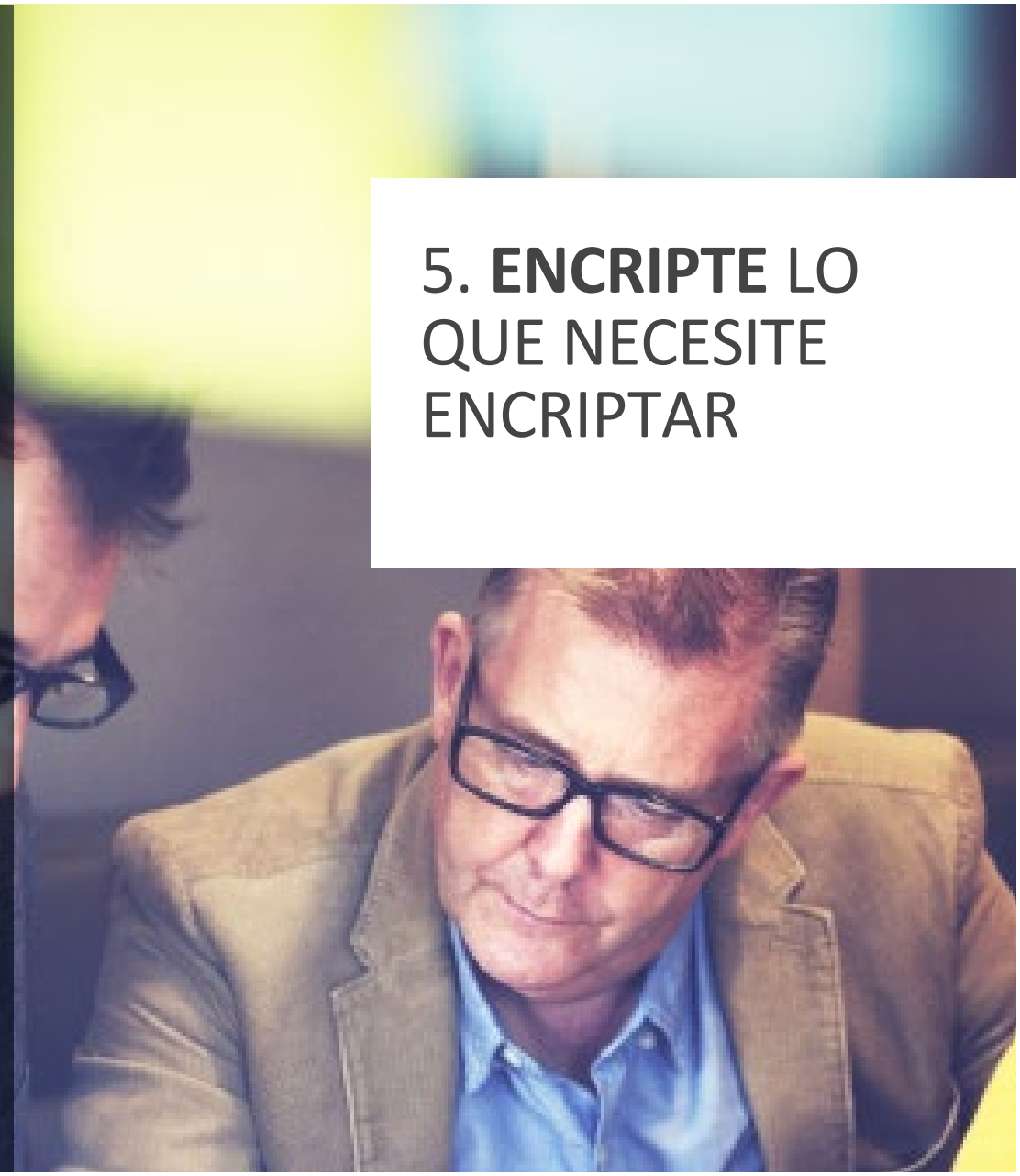


MANTÉNGASE LEJOS DE LOS HACKERS

Puede explorar los patrones de ataque y aplicar todas las políticas que desee, pero con nuevas vulnerabilidades expuestas aparentemente a diario, tendrá dificultades para enfrentarse a todas ellas. Aunque la administración de parches no es una bala de plata y no prevendrá de todos los abusos, de hecho, pueden haver vulnerabilidades aún sin parchear, le ayudará a mantener araya a los hackers.

Una buena regla es suscribirse a las notificaciones de los proveedores, vigilar los sitios de noticias de seguridad, y actualizar tan pronto como sea seguro hacerlo. Ahí es donde la gestión de parches entra en la ecuación, ya que no sólo debe saber que hay un parche disponible, sino también que éste es estable. Lanzar un parche inestable en su entorno de trabajo sin realizar pruebas podría hacer más daño a la línea de flotación del negocio que el *exploit* que está tratando de evitar.

5. **ENCRIPTE** LO QUE NECESITE ENCRIPTAR



FOCALIZARSE EN LOS DATOS QUE SON MÁS VALIOSOS

El problema con el cifrado de datos es que casi siempre se ve como un paso demasiado complejo, demasiado caro, demasiado... La verdad es que si usted identifica los datos que son más valiosos para su organización y luego se centran en cifrarlos, no tiene porqué ser así.

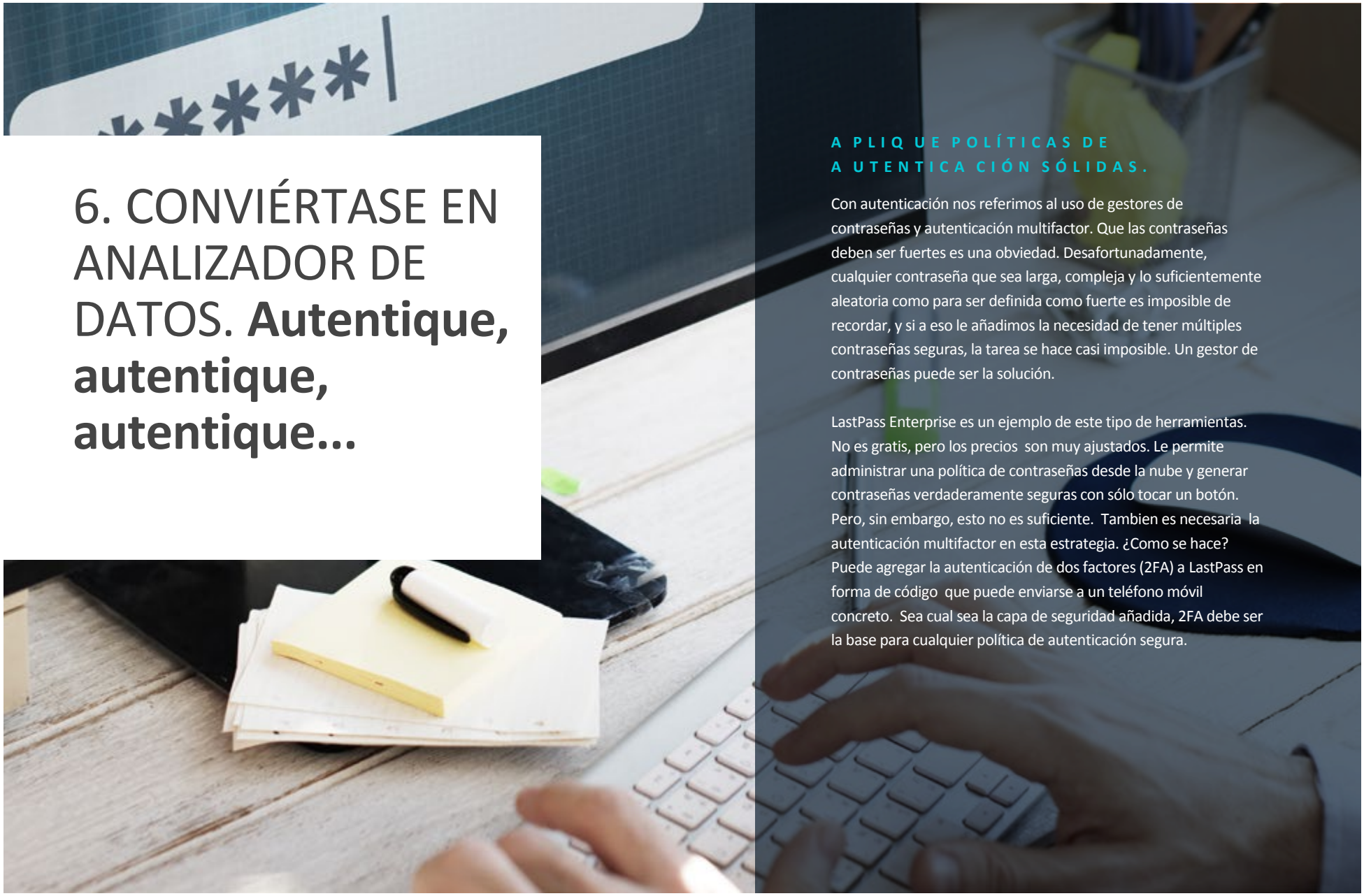
Los datos que se cifran con suficiente fuerza estarán más allá de las capacidades de la mayoría de los hackers. Y no es nada difícil. Asegúrese de revisar lo siguiente:

• Tabletas y teléfonos inteligentes: el cifrado de firmware incorporado en el sistema operativo los hace inútiles para los ladrones. Utilícelo.

• Sitios web: Protocolo de transferencia de hipertexto seguro (HTTPS) cifra la información transferida entre él y los navegadores de cliente.

• Navegadores web: HTTPS Everywhere es una extensión para navegadores que reescribe solicitudes de sitios HTTP sin cifrar para securizarlos.

• Memory Stick USB: VeraCrypt se ha convertido en el producto de encriptación de código abierto estrella. Es fácil de usar, funciona, y es gratis.

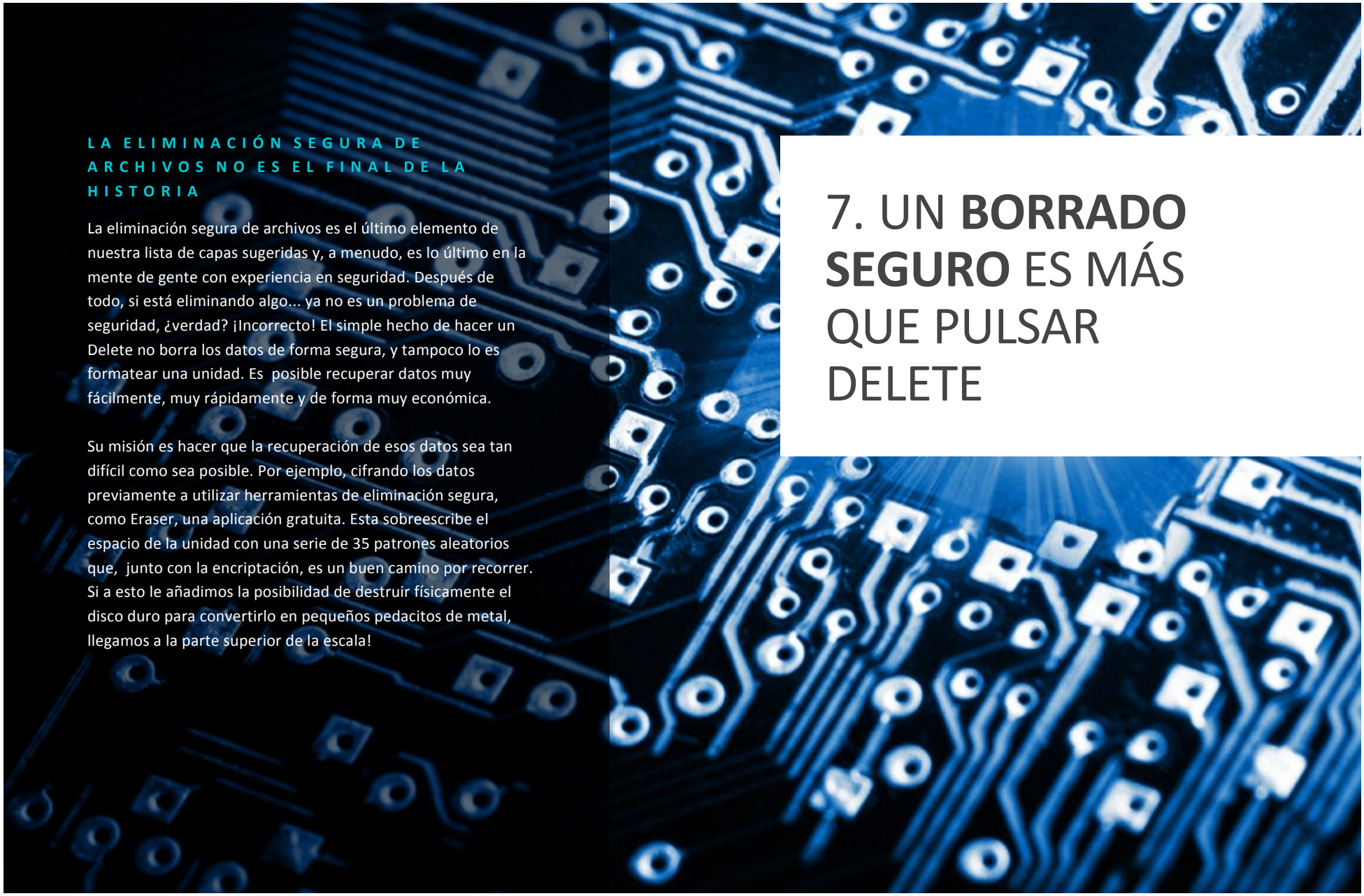


6. CONVIÉRTASE EN ANALIZADOR DE DATOS. **Autentique, autentique, autentique...**

A PLIQ UE POLÍTICAS DE A UTENTICA CIÓN SÓLIDAS.

Con autenticación nos referimos al uso de gestores de contraseñas y autenticación multifactor. Que las contraseñas deben ser fuertes es una obviedad. Desafortunadamente, cualquier contraseña que sea larga, compleja y lo suficientemente aleatoria como para ser definida como fuerte es imposible de recordar, y si a eso le añadimos la necesidad de tener múltiples contraseñas seguras, la tarea se hace casi imposible. Un gestor de contraseñas puede ser la solución.

LastPass Enterprise es un ejemplo de este tipo de herramientas. No es gratis, pero los precios son muy ajustados. Le permite administrar una política de contraseñas desde la nube y generar contraseñas verdaderamente seguras con sólo tocar un botón. Pero, sin embargo, esto no es suficiente. Tambien es necesaria la autenticación multifactor en esta estrategia. ¿Como se hace? Puede agregar la autenticación de dos factores (2FA) a LastPass en forma de código que puede enviarse a un teléfono móvil concreto. Sea cual sea la capa de seguridad añadida, 2FA debe ser la base para cualquier política de autenticación segura.



7. UN **BORRADO SEGURO** ES MÁS QUE PULSAR DELETE

LA ELIMINACIÓN SEGURA DE ARCHIVOS NO ES EL FINAL DE LA HISTORIA

La eliminación segura de archivos es el último elemento de nuestra lista de capas sugeridas y, a menudo, es lo último en la mente de gente con experiencia en seguridad. Después de todo, si está eliminando algo... ya no es un problema de seguridad, ¿verdad? ¡Incorrecto! El simple hecho de hacer un Delete no borra los datos de forma segura, y tampoco lo es formatear una unidad. Es posible recuperar datos muy fácilmente, muy rápidamente y de forma muy económica.

Su misión es hacer que la recuperación de esos datos sea tan difícil como sea posible. Por ejemplo, cifrando los datos previamente a utilizar herramientas de eliminación segura, como Eraser, una aplicación gratuita. Esta sobreescribe el espacio de la unidad con una serie de 35 patrones aleatorios que, junto con la encriptación, es un buen camino por recorrer. Si a esto le añadimos la posibilidad de destruir físicamente el disco duro para convertirlo en pequeños pedacitos de metal, llegamos a la parte superior de la escala!

Necesita más ayuda?

ontek@ontek.net

902 566 048

www.ontek.net

OnTek