+ Windows 10

EL MANUAL DE CIBER-SEGURIDAD

Diez pasos que todo negocio debe dar para protegerse de los ciberataques.

Protéjase desde el encendido al apagado.

El entorno de la ciberseguridad está cambiando y expandiéndose constantemente. Las pequeñas y medianas empresas tienen que enfrentarse cada vez más a ciberataques que amenazan su información y la privacidad de los datos de sus clientes. Esta guía está diseñada para ayudar a esas pequeñas y medianas empresas con recursos informáticos limitados a mejorar su ciberseguridad hoy mismo, con poco o ningún coste.

ÍNDICE

El entorno de riesgo

Las tendencias en ciberseguridad en las pequeñas y medianas empresas

Estas son las cinco tendencias principales en relación con la ciberseguridad para pequeñas y medianas empresas, según el Ponemon Institute[1]:

1. **Cada vez se atacan más negocios.**
En los últimos 12 meses, los ciberataques a pequeñas y medianas empresas han aumentado un 11 %, del 55 al 61 por ciento. Los ataques más comunes contra pequeñas empresas son phishing/ingeniería social (48 %) y los basados en la web (43 %). Al mismo tiempo, los ciberataques cada vez son más específicos, severos y sofisticados.

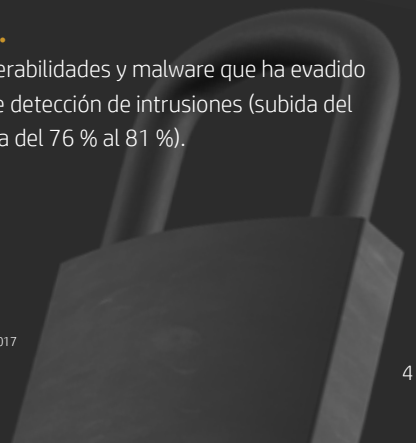
2. **Los ataques cada vez son más costosos.**
El coste medio debido a la interrupción de las operaciones normales aumentó un 26 %, de 955 429 a 1 207 965 $. El coste medio debido a daños o robo de activos e infraestructura informática aumentó de 879 582 a 1 027 053 $.

3. **Los errores humanos son una de las causas principales.**
De las pequeñas y medianas empresas que sufrieron una vulneración de datos, el 54 % dicen que la causa principal fueron empleados descuidados, un aumento del 48 % del año pasado. Sin embargo, igual que el año pasado, 1 de cada 3 empresas en esta investigación no pudieron determinar la causa principal.

4. **Las contraseñas fuertes y la autenticación multifactor siguen sin utilizarse lo suficiente.**
Las contraseñas siguen siendo una parte integral de la ciberseguridad. Sin embargo, el 59 % de los participantes dicen que no tienen visibilidad de las prácticas de contraseñas de sus empleados, como el uso de contraseñas únicas o fuertes y el compartir contraseñas con otras personas; esto no ha cambiado desde el año pasado.

> El 59 % dicen que no tienen visibilidad en las prácticas de contraseñas de sus empleados

5. **El malware cada vez es más sofisticado.**
Cada vez más empresas son víctimas de vulnerabilidades y malware que ha evadido las protecciones existentes, como sistemas de detección de intrusiones (subida del 57 % al 66 %) y soluciones de antivirus (subida del 76 % al 81 %).



1—Informe: 2017 State of Cybersecurity in Small & Medium-Sized Businesses. Ponemon Institute LLC, 2017

Los cinco ataques más comunes contra pequeñas y medianas empresas.

1

Phishing/ingeniería social

El phishing es una forma de ingeniería social. En un ataque de phishing, el atacante finge ser una organización de confianza y utiliza el correo electrónico o sitios web maliciosos para solicitar información personal.[2]

2

Ataques basados en la web

En los ataques basados en la web, el atacante obtiene acceso a un sitio web legítimo y envía malware. El sitio legítimo actúa como un organismo huésped, infectando a los visitantes confiados. Uno de los tipos más perniciosos de ataques basados en la web es la "descarga en movimiento", en la que el contenido malicioso se descarga automáticamente en el ordenador de un usuario que solo navegaba por el sitio. No es necesaria la interacción con el usuario.[3]

3

Malware

Malware es un término general que se refiere a cualquier software diseñado intencionadamente para causar daño a un dispositivo o red.[4] Esto incluye virus, spyware, ransomware y todos los "ware". Más allá de los ataques basados en la red, puede entrar al ordenador de una víctima a través de un dispositivo USB o una conexión de red comprometida.[5]

4

Dispositivos comprometidos/robados

Un dispositivo que haya sido comprometido o robado puede contener tanto información de valor como credenciales guardados localmente que puedan permitir mayor acceso a la información y redes de la organización. Las contraseñas débiles y el cifrado de datos pueden agravar este tipo de ataques.

5

Ataques de denegación de servicio

Los ataques de denegación de servicio se consiguen inundando la red atacada con tráfico, hasta que no pueda responder o se caiga, evitando el acceso de usuarios legítimos. Un ataque de denegación de servicio distribuido (DDoS por sus siglas en inglés) ocurre cuando hay varias máquinas operando a la misma vez para atacar un objetivo, aumentando el poder del ataque. Los DDoS también aumentan la dificultad de encontrar la verdadera fuente.[6]

2—https://www.us-cert.gov/ncas/tips/ST04-014
3—https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/web-based-attacks-09-en.pdf
4—https://technet.microsoft.com/en-us/library/dd632948.aspx
5—https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf
6—https://www.us-cert.gov/ncas/tips/ST04-015

10 maneras de protegerse

Sección 1:

Habilite la autenticación por multifactor

Los nombres de usuario y contraseñas son los objetivos clave de los hackers, y con razón: su identidad es su bien más valorado. Las contraseñas fuertes y seguras ayudan, pero ellas solas no son el mecanismo de autenticación más seguro. Y en un mundo en el que la piratería está cada vez más comercializada, los ladrones que no sean expertos pueden externalizar ese trabajo. Los hackers pueden construir hardware diseñado especialmente para descifrar contraseñas, alquilar espacio de proveedores de nube privados o crear botnets para que lleven a cabo el procesamiento.

- El 90 % de los datos robados con phishing son credenciales de usuario[7]
- El 80 - 90 % de las contraseñas se pueden hackear en menos de 24 horas[8]

La autenticación por multifactor (MFA por sus siglas en inglés) requiere que use dos o más credenciales independientes para demostrar su identidad, aumentando de manera sustancial su nivel de seguridad. Las credenciales pueden ser algo que el usuario **conozca** (contraseñas o PIN), algo que **tenga** (teléfonos Bluetooth® o tarjetas inteligentes) o algo que **sea** (reconocimiento facial o táctil). Si un factor se ve comprometido o se rompe, el atacante todavía tiene que enfrentarse a un segundo tipo de barrera diferente.

HP MFA e Intel® Authenticate permiten que la autenticación por múltiple factor sea necesaria con cada intento de inicio de sesión.

7—Verizon, 2016 Data Breach Investigations Report, 2016
8—Fuente: Brian Contos, CISO de Verodin, Inc. Citado con permiso. https://www.csoonline.com/article/3236716/authentication/how-hackers-crack-passwords and-why-you-cant-stop-them.html

Configure autenticación por multifactor con HP.

Los dispositivos Modern HP Pro o Elite permiten configurar MFA mediante HP Client Security Manager.[9]

1. Abra Client Security Manager (necesitará acceso de administrador). Si lo abre dentro del Manageability Integration Kit (MIK) de HP, puede enviar sus políticas de MFA a toda su flota de ordenadores.[10]
2. Desde el panel de control, haga clic en Políticas de usuario estándar.
3. Elija dos o tres factores para configurar una política de inicio de sesión y siga las instrucciones para registrar la credencial o el par de credenciales, como escanear su huella dactilar desde el lector de huellas del ordenador o introducir un código PIN.

Diversifique con Windows Hello.

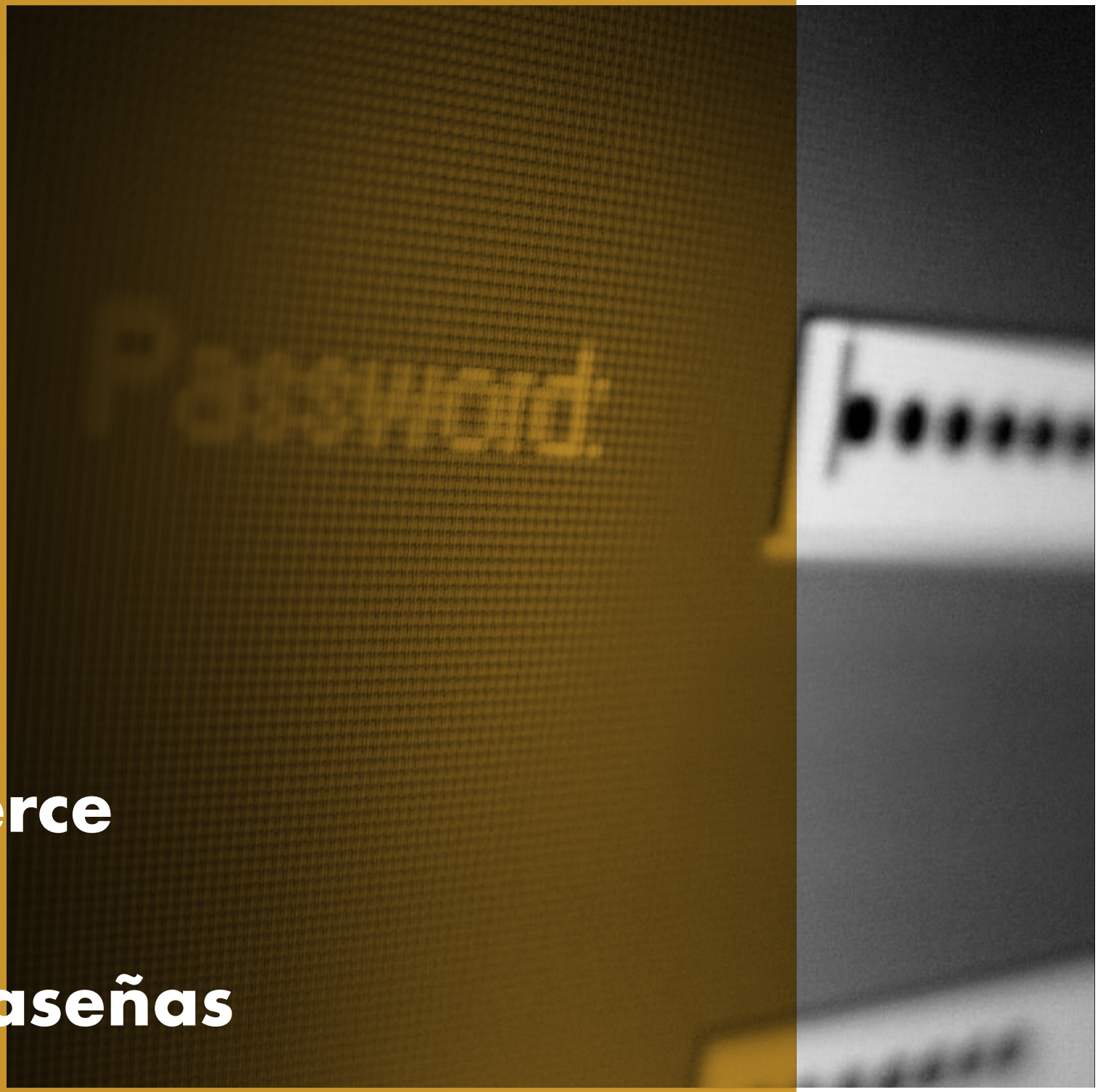
Muchos dispositivos modernos de Windows 10 Pro con webcam integrada son compatibles con Windows Hello, entre ellos toda la gama de portátiles y convertibles de HP. Al escanear su rostro, Windows Hello proporciona una alternativa a la contraseña como una de sus credenciales MFA.

1. Abra Configuración > Cuentas > Opciones de inicio de sesión
2. En “PIN” seleccione “Añadir”, si no ha establecido ya uno.
3. En “Windows Hello” seleccione “Establecer” y siga las instrucciones en la pantalla para escanear su rostro.

9—HP Client Security Manager Gen4 requiere Windows y procesadores Intel® o AMD de 8.ª generación.
10—HP Manageability Integration Kit puede descargarse en http://www.hp.com/go/clientmanagement.

Sección 2:

Refuerce sus contraseñas



Las contraseñas están siempre presentes en nuestra vida cotidiana. Las usamos para prácticamente todos los dispositivos, servicios y cuentas personales o profesionales. Como son la primera (y muchas veces la única) línea de defensa en la protección de nuestros datos e identidad, utilizar una mala contraseña puede tener terribles resultados. A pesar de esto, la mayoría de personas no utilizan contraseñas fuertes y únicas.

- El 59 % sabe que una contraseña segura es importante, pero solo el 41 % elige una contraseña que sea fácil de recordar
- El 91 % entiende el riesgo de reutilizar contraseñas, pero el 55 % lo sigue haciendo
- Los milenials suelen utilizar contraseñas más seguras que los Baby Boomers (65 % vs. 45 %)[11]

Si su dispositivo o servicio no es compatible con MFA, la siguiente mejor opción es crear una contraseña que funcione lo mejor que sea posible. La mayoría de la gente no tiene contraseñas fuertes porque no entienden cómo crearlas, asumiendo que lo mejor es una combinación arbitraria de letras, números y símbolos. Pero hay maneras mejores y más sencillas de aumentar enormemente el nivel de protección de su contraseña.

11—Fuente: LastPass, "New Research: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, 1 de mayo de 2018

La nemotecnia antes que los números.

Las frases de contraseña nemotécnica son más seguras que las contraseñas simples y más fáciles de recordar que las numéricas.
Cuando se usan en vez de contraseñas sencillas, las frases de contraseñas nemotécnicas son prácticamente imposibles de descifrar por los hackers.

1 Empiece con una frase memorable.

Por ejemplo, las cinco primeras palabras del famoso discurso de Gettysburg de Abraham Lincoln, “Hace ochenta y 7 años”, son una frase de contraseña sencilla. Esta frase cumple la mayoría de normas de contraseñas: 8-32 caracteres de longitud e incluye letras mayúsculas y minúsculas y al menos un número y un carácter especial (los espacios, o guiones si no se permiten los espacios).

2 Maximice las rarezas.

Aumente la cantidad de números y caracteres especiales que utiliza. Por ejemplo, modifique las letras en el ejemplo anterior para escribir: "Hace ochent@ & 7 @ño$".

3 Personalice, no copie.

Al adjuntar un sufijo sencillo al final de cada frase de contraseña, puede reutilizar su contraseña maestra fácilmente sin el peligro de usos duplicados. Para una cuenta de Facebook, pruebe a añadir “FB” al final de la frase de contraseña, o “IG” para Instagram.

Utilice un gestor de contraseñas.

Los gestores de contraseñas son una de las prácticas de seguridad más recomendadas por los expertos en seguridad. Funcionan generando y guardando contraseñas largas y complicadas para cada una de sus cuentas en línea, liberándole de tener que recordarlas. En general, solo tendrá que recordar una contraseña: la contraseña maestra a su "caja fuerte". La configuración del gestor es fácil y el proceso suele ser el mismo:

1. Descargue e instale el software y una extensión para su navegador. También puede descargarse una aplicación para su dispositivo móvil.
2. Configure su cuenta con un correo electrónico y su contraseña maestra.
3. Introduzca los detalles de sus diferentes cuentas.

La mayoría de los gestores de contraseñas le pedirán que actualice manualmente sus contraseñas antiguas: inicie sesión en su cuenta, vaya a los ajustes de su cuenta y deje que el gestor de contraseñas genere una contraseña nueva más segura. Reemplazar sus antiguas contraseñas puede llevar tiempo, pero el aumento de seguridad hará que valga la pena.

Elegir un gestor de contraseñas.

Existen numerosos gestores de contraseñas gratuitos, incluidos Bitwarden, Dashlane y Enpass. En general, busque un gestor de contraseñas que:

- Se integre fácilmente en el navegador que más utilice
- Le permita guardar el archivo de contraseñas como un archivo cifrado, que no pueda ser leído por usuarios sin verificar su identidad. Específicamente, elija un gestor de contraseñas que use cifrado AES-256 o más fuerte.
- Permita la autenticación de 2 factores para acceder a la caja fuerte de contraseñas.
- Asigne un contacto de emergencia que también pueda tener acceso a la caja fuerte de contraseñas.
- Guarde información de inicio de sesión adicional junto con la contraseña (por ejemplo, preguntas de seguridad, números de teléfono, información de la cuenta, etc...)

Sección 3:

Utilice un software antimalware

Sin protección antivirus, un malware podría infectar un PC en pocos minutos de conexión a Internet.

Malware de todo tipo se puede hospedar en sitios que parecen respetables o en adjuntos de correos electrónicos, y cada día se crea malware nuevo. El bombardeo de virus a su PC es constante, así que una herramienta que lo proteja debe ser fuerte, arraigada y se debe actualizar regularmente. Un buen programa antimalware es estas tres cosas.

En resumen, el software antimalware es un programa o un conjunto de programas diseñados para evitar, buscar, detectar y eliminar virus de software (y otro software maligno como gusanos, troyanos, adware y muchos más). Un programa antimalware típico escaneará su sistema regularmente y eliminará automáticamente el malware que encuentre, y le alertará de descargas peligrosas y actualizaciones de software.

Consígalo si aún no lo tiene.

Existen muchos productos antimalware disponibles. Si trabaja con Windows 10 Pro en su PC, ya tiene el programa Antivirus de Windows Defender instalado y funcionando. De forma alternativa, puede comprar un programa antimalware de terceros. Pero asegúrese de seguir las instrucciones del proveedor para configurar las actualizaciones automáticas, para que siempre tenga la protección de virus más actualizada.

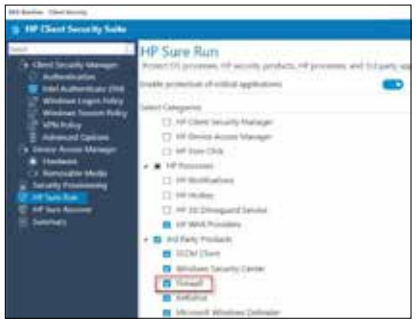
Ejecútelo en todo momento.

Aún más importante, el software antimalware debe ejecutarse en todo momento para seguir siendo efectivo. Como es normal que los atacantes de malware ataquen primero los programas de seguridad como el antimalware, este paso no es tan sencillo como parece. En Windows 10 Pro, puede verificar si su programa antivirus está habilitado actualmente comprobando el Centro de seguridad de Windows Defender.

1. Desde el menú de Inicio, abra el Centro de seguridad de Windows Defender y vaya a Inicio.

2. En “Protección antivirus y contra amenazas”, si el antivirus se está ejecutando, verá una marca de verificación verde. Si utiliza un programa antivirus de terceros, haga clic en “Ver proveedores de antivirus” para ver detalles adicionales de seguridad en el Panel de control de Windows sobre el estado de su programa antivirus.

Y siga ejecutándolo.



Los productos HP Elite también incluyen HP Sure Run[12], una capa extra de seguridad que asegura que todos los procesos críticos de su PC, incluido el software antivirus, siguen ejecutándose. Cualquier proceso que controle Sure Run se reiniciará automáticamente si se deshabilita, evitando que un software antivirus deshabilitado o caído le deje vulnerable.

HP Sure Run debe estar habilitado localmente en HP Client Security Manager Gen4.

12—HP Sure Start está disponible en los productos HP Elite equipados con procesadores Intel® o AMD® de 8.ª generación.

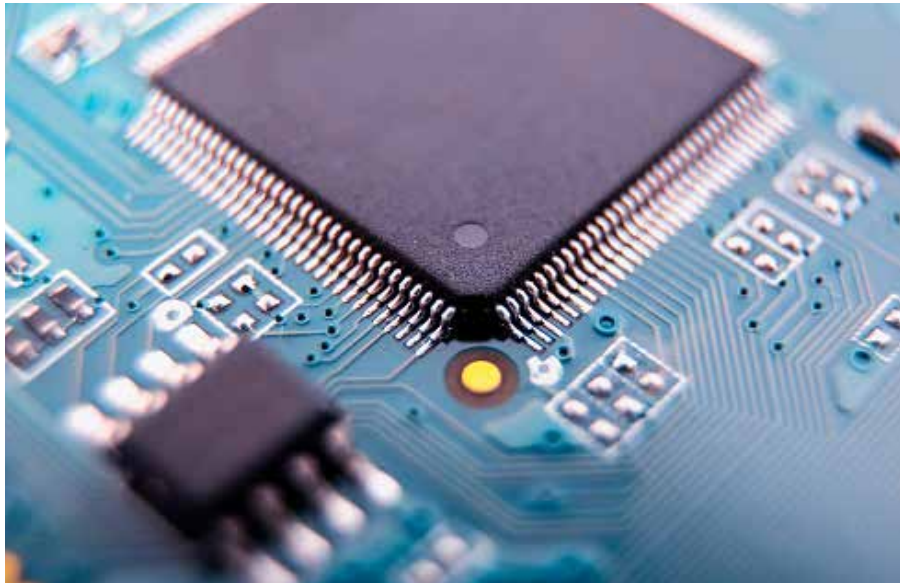
Sección 4:

Mantenga su software al día

El antimalware no es el único software que se enfrenta a riesgos cambiantes; es importante mantener todo su software al día. Si su software no está actualizado, pueden faltarle parches de seguridad importantes para vulnerabilidades recién descubiertas. Esto se aplica tanto al sistema operativo (SO), como Windows®, como a todas las aplicaciones ejecutadas en su PC, como navegadores de Internet, aplicaciones de Office, software de contabilidad, antivirus, etc.

El usuario debe tener en cuenta que puede que el software más antiguo o descontinuado ya no reciba las actualizaciones de seguridad. Conforme pasa el tiempo, los cibercriminales encuentran vulnerabilidades en software publicado y se aprovechan de estos descubrimientos. Usando el SO como ejemplo, buscar una actualización para Windows 7 Pro puede no presentar ningún software nuevo, pero esto pasa por alto que Windows 7 Pro ya no es la versión más actual de Windows. Parchear software antiguo no es lo mismo que actualizar a la última versión: cuanto más antiguo sea su software, menos seguro será.

> Cuanto más antiguo sea el software, menos seguro será



Compruebe que está actualizado.

Cuando los proveedores de software encuentran soluciones a las vulnerabilidades, envían esas soluciones mediante las actualizaciones de software. La mayoría de las aplicaciones tienen un servicio de actualizaciones integrado en su software, lo que garantiza que se le notificará cuando haya una actualización o parche disponible. Algunos proveedores de software incluso instalan automáticamente las actualizaciones cuando están disponibles.
Windows 10 Pro, el último lanzamiento de Windows (y por lo tanto el más seguro), tiene un mecanismo de actualización de software automatizado para mantener el sistema operativo al día, y todas las aplicaciones de Microsoft, como Microsoft Office, también.

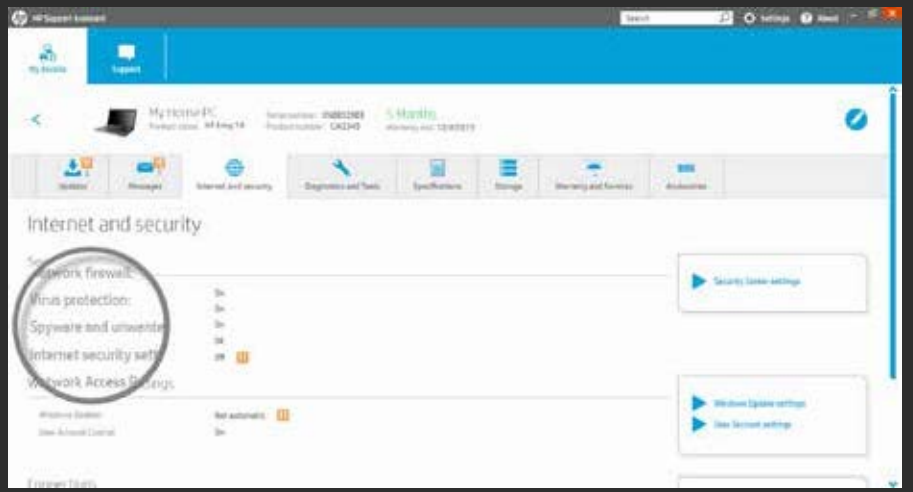
Para comprobar si las actualizaciones automáticas están habilitadas:

1. Vaya a ajustes y seleccione “Actualizar seguridad”.
2. En “Actualización de Windows” elija “opciones avanzadas” y asegúrese de que “Automáticamente” está seleccionado en “Elija cómo se instalan las actualizaciones”.
3. Asegúrese de que “Automáticamente” está seleccionado en “Elija cómo se instalan las actualizaciones”.

Utilice un gestor de actualizaciones.

La variedad de software que viene con su PC puede hacer que sea difícil asegurarse de que *todo* está al día. Por eso, muchos proveedores de PC proporcionan herramientas preinstaladas para recopilar automáticamente todas las actualizaciones de software y firmware para el sistema. En los sistemas HP, esta herramienta se llama HP Support Assistant.

Para aplicaciones de terceros, la función de actualización la realiza normalmente una pequeña aplicación de actualizaciones que se inicia con el arranque. Esta herramienta hace que el arranque dure unos segundos más, pero le ahorra tener que buscar actualizaciones en los sitios webs de los proveedores de la aplicación. Si tiene un software que no busca actualizaciones automáticamente, o si no está seguro, compruebe el número de versión en el sitio web del desarrollador y actualice para que coincida, si es necesario.



Sección 5:

Proteja su navegador

Los navegadores, como Internet Explorer o Chrome™, son la manera principal con la que accedemos a Internet, lo que les convierte en el objetivo n.º 1 de los hackers. Estos ataques llegan normalmente al hacer clic de manera accidental o intencionada en un enlace que desata un código malicioso, conocido como malware.

Puede realizar una serie de pasos sencillos para reducir de manera significativa las posibilidades de un ataque de malware a través de su navegador.

Utilice un navegador seguro.

Internet Explorer, Edge y Chrome ofrecen características de seguridad sólidas para Windows. Edge e Internet Explorer 11, por ejemplo, utilizan Microsoft SmartScreen para realizar un control de reputación de cada sitio y bloquear cualquiera que sospechen que pueda ser un sitio de phishing. Además, en los ordenadores comerciales de HP, Internet Explorer se beneficia de la seguridad adicional de HP Sure Click, que ejecuta cualquier pestaña abierta en una máquina virtual aislada. Esto significa que cualquier código malicioso se atrapa en la pestaña y se destruye cuando cierre su navegador[13].

Preste atención a los avisos.

La mayoría de navegadores modernos tienen un umbral básico para detectar sitios web maliciosos y le mostrarán un aviso si creen que hay una amenaza razonable. Algunos también ofrecen funciones de autocorrección, para evitar navegar a un dominio que se suela escribir mal (donde se hospedan normalmente software y sitios web maliciosos).

En Edge, vaya a Configuración avanzada> Privacidad y habilite “Usar un servicio web para ayudar a resolver errores de navegación”

Manténgalo actualizado.

Permita las actualizaciones automáticas de navegador en la Configuración. Como se ha mencionado anteriormente, esto le asegurará que se aplican todas las actualizaciones de seguridad a su navegador, haciéndolo más seguro y aumentando la posibilidad de que fallen los ataques de malware.

En Edge, las actualizaciones se aplican cada vez que se actualiza Windows. Sin embargo, para comprobar si necesita un actualización para Edge, vaya a

- Inicio
- Configuración
- Actualizaciones y seguridad
- Windows Update
- Buscar actualizaciones

Limite contenidos y plug-ins.

Muchos de estos complementos para navegador (como Flash o JavaScript) son necesarios para sitios y programas web enriquecidos, pero el acceso cada vez mayor a su sistema también los convierte en un punto vulnerable.

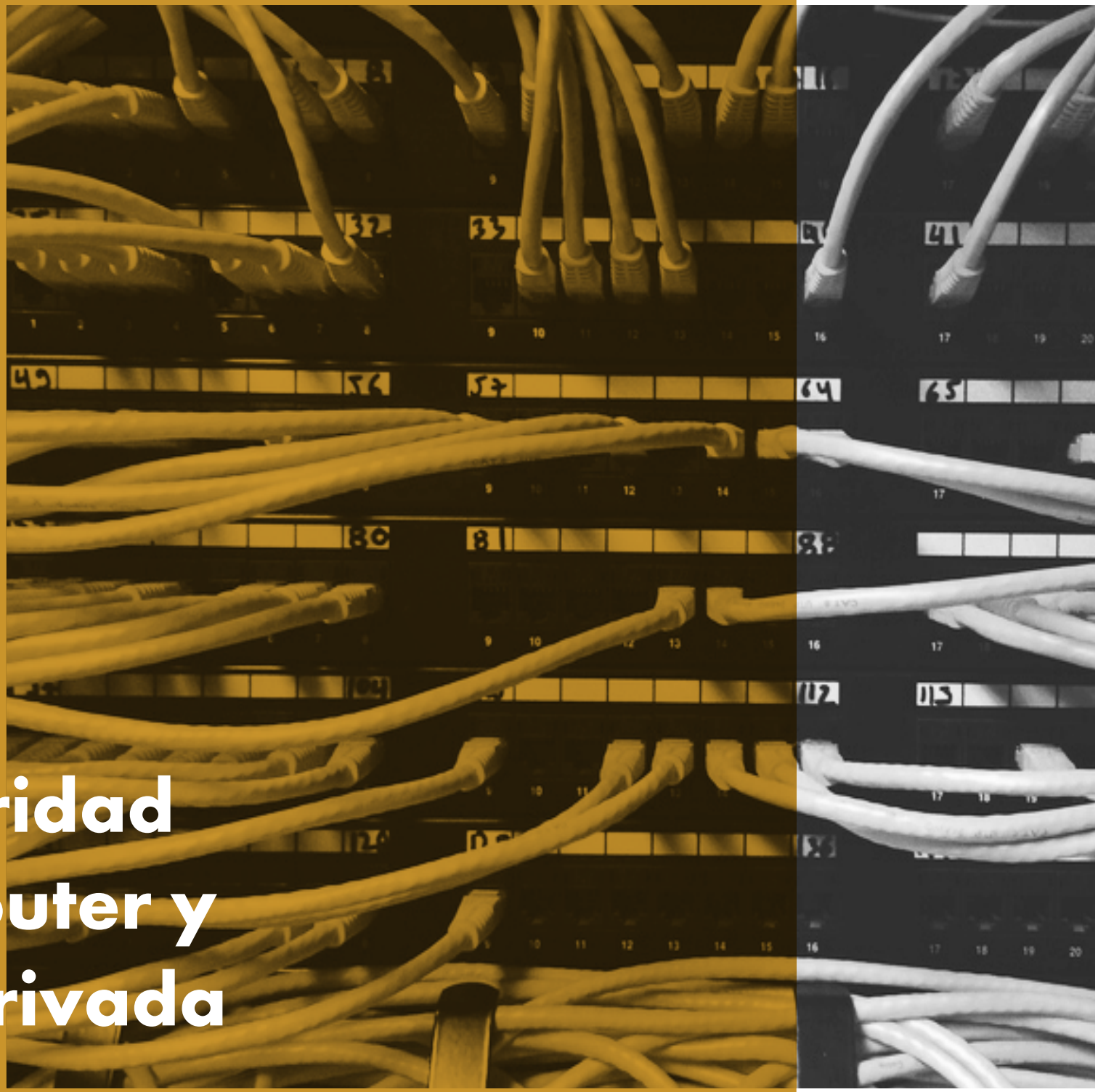
Desactivarlos por defecto hace que un sitio deba pedir permiso para usarlos y asegura que solo los sitios en los que usted elige confiar pueden usar sus funciones.

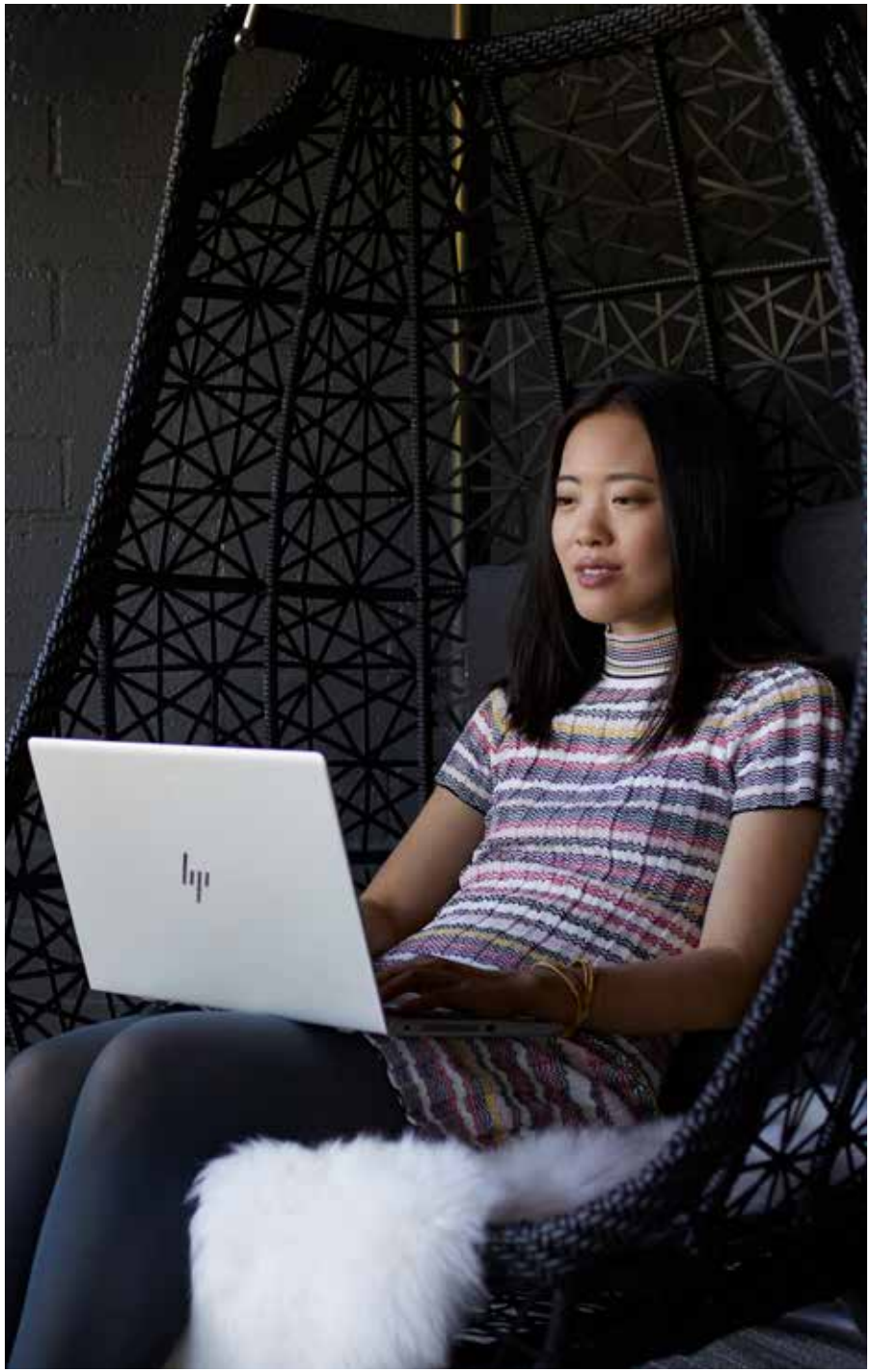
En IE, vaya a Herramientas (icono de engranaje) > Opciones de Internet > Seguridad > Internet > Nivel de cliente... > Scripting. Puede deshabilitar JavaScript seleccionando “Deshabilitar” o puede pedir a IE que le pregunte antes de que un sitio intente usarlo, seleccionando “Pedir confirmación”.

13—HP Sure Click está disponible en la mayoría de los ordenadores HP y es compatible con Microsoft® Internet Explorer y Chromium™. Los adjuntos compatibles incluyen Microsoft Office (Word, Excel, PowerPoint) y archivos PDF solo en modo de lectura, cuando Microsoft Office o Adobe Acrobat están instalados.

Sección 6:

Seguridad del router y red privada





El router es la primera capa de seguridad ante la intrusión a cualquier red. Cualquier persona que se conecta a Internet lo hace a través de un router. Este dispositivo hardware, con o sin cable (Wi-Fi®), le permite comunicarse entre su red local (por ejemplo, su PC y otros dispositivos conectados) e Internet. Por lo tanto, habilitar el nivel más alto de seguridad en el router es la mejor manera de mantener su ordenador, sus impresoras y sus datos seguros ante un ataque malicioso.

> Los routers se convierten en el tipo de dispositivo más explotado en ataques al Internet de las cosas.[14]

Ya que el router transmite TODOS los datos que entran y salen de su casa o negocio, incluidos el correo electrónico y la información de tarjeta de crédito, ha sido el objetivo favorito de los hackers desde hace mucho tiempo. En el 2018 Internet Security Threat Report de Symantec, se cita a los routers como el tipo de dispositivo más explotado en ataques al Internet de las cosas. Los hackers pueden usar malware o diseñar errores para ocultar su identidad, robar ancho de banda, convertir sus dispositivos en zombies botnets, o acciones aún peores. También pueden aprovechar cualquier dispositivo no seguro.

14—Fuente: Symantec Corporation, 2018 Internet Security Threat Report, 2018

Proteja su red.

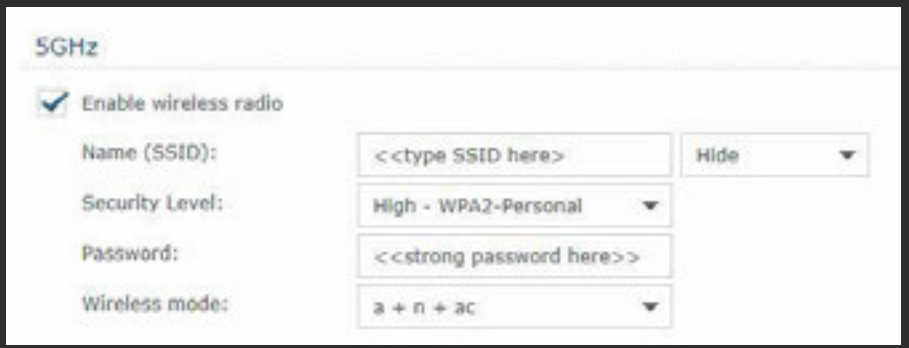
Por desgracia, muchos proveedores siguen ofreciendo configuraciones de router tanto inseguras como seguras. Si un router no es seguro (es decir, permite conexiones sin que sea necesaria la contraseña de administrador), cualquier persona podría conectarse a él y entrar a su red local. Un hacker podría cambiar las contraseñas, espiarle e incluso acceder a sus archivos en un disco duro conectado a la red.

Proteja siempre sus routers con contraseñas de administrador que no sean por defecto, utilizando los consejos de la Sección 2: Refuerce sus contraseñas. A continuación hay una captura de pantalla de cómo le permiten establecer contraseñas la mayoría de routers para asegurarlos en la red.

Configure el cifrado.

Con los routers inalámbricos, las contraseñas son solo la mitad de la batalla: elegir el nivel adecuado de cifrado es igual de importante. La mayoría de los routers inalámbricos son compatibles con cuatro normas de cifrado inalámbrico: WEP (la más débil), WPA (fuerte), WPA2 (más fuerte) y WPA3 (la más fuerte). Opte por la norma de cifrado más fuerte compatible con su enrutador.

A continuación le mostramos una captura de pantalla para establecer el nivel apropiado de cifrado en su router. Para ello, debe iniciar sesión como administrador del router y navegar a la configuración de cifrado (varía según el proveedor de router).



Mantenga el firmware actualizado.

Muchos fabricantes de routers lanzan actualizaciones de software a lo largo del año para abordar problemas de seguridad. Como explicamos con el software de PC, es mucho menos probable que un router con las últimas actualizaciones se infecte con malware. La mayoría de los proveedores de routers aplican actualizaciones de firmware automáticas sin que los clientes tengan que realizar esta operación. Los nuevos modelos de routers también pueden ofrecer una aplicación móvil, que se puede descargar a su ordenador como cualquier otra aplicación, y usarla para buscar actualizaciones. Sin embargo, si el proveedor de su router no ofrece actualizaciones de firmware automáticas, debe ir al sitio web del fabricante, ir a Ayuda e identificar la actualización correcta según el nombre específico del modelo e ID (normalmente se encuentra en el router).

Utilice redes privadas virtuales.

Una red privada virtual va más allá de la seguridad del hardware dentro de su empresa, se trata de un servidor al que se conecta para reenrutar sus actividades de Internet externas. La VPN puede proteger y asegurar su identidad e información. El objetivo de una VPN es proporcionar una manera general de navegar la web de manera privada (pero no siempre anónima). Todo el tráfico que pasa a través de su conexión de VPN es seguro y no puede, en teoría, ser interceptado por nade más. Es decir, son ideales para usar tanto en redes locales como públicas. Más información sobre VPN y sus ventajas en la Sección 7.

Sección 7:

Protéjase en la Wi-Fi® pública

Hoy, la Wi-Fi® pública es casi universal. Los aeropuertos, bares locales, centros comerciales, incluso los parques ofrecen acceso Internet gratuito a través de puntos de conexión. Son muy cómodos... y peligrosos.

Los usuarios conectados a estos puntos comparten la misma red, lo que significa que hay muchas probabilidades de que alguien pueda aprovecharse de este tráfico no seguro. Un hacker podría incluso configurar un punto de conexión para atraer a gente a su red falsa (con un nombre parecido). Esto permite interceptar flujo de datos sin cifrar o ejecutar los ataques de intermediario para sortear el cifrado.

Es importante asumir siempre que sus comunicaciones son públicas y no seguras cuando usa una red pública. Sin embargo, si no hay otra opción, hay maneras de reducir su exposición.

Limite su actividad.

No transmita material que sea muy sensible, como documentos de empresa, correos electrónicos o contraseñas, y no utilice ningún tipo de aplicaciones o portales de banca/contabilidad.

Busque un plan B.

Si es posible, utilice redes semiabiertas, que estén protegidas al menos con contraseñas. Normalmente, suelen ser redes gestionadas, es decir, el proveedor tiene interés en mantener la red segura (p. ej., salas de aeropuerto)

Quédese en sitios cifrados.

Asegúrese que está conectado a un servidor web que sea compatible con el tráfico cifrado a través de un protocolo HTTPS (https://), en lugar del protocolo HTTP de texto sencillo y no seguro. Compruebe el encabezado de la URL del sitio: un navegador moderno normalmente tendrá un icono en la barra de URL que indica cuando el HTTPS está presente y que certifica que es válido (suele ser un icono de candado o el color verde). Hacer clic en esa zona abrirá un diálogo que dará más información sobre el nivel de cifrado.

Enrútelo todo a través de una VPN.

Como mencionamos anteriormente, una VPN puede ayudar a proteger sus datos cuando no se puede fiar de la red de conexión; y una red Wi-Fi® es el ejemplo perfecto. Un túnel VPN cifra sus datos de extremo a extremo, asegurando que un posible interceptor no sea capaz de interpretar su actividad. Pero no todas las VPN son iguales, así que deberá elegir la mejor opción para usted según su presupuesto y su tipo de dispositivo. Las VPN gratuitas suelen tener ancho de banda limitado y protocolos de cifrado sencillos, por lo que experimentará una velocidad de navegación más lenta, y todavía podría quedar expuesto. Dicho esto, en resumen, una VPN gratuita respetable sigue siendo mejor que no usar VPN.

Sección 8:

Pare a los hackers visuales

La piratería visual ocurre cuando se muestra información sensible en la pantalla en espacios públicos y la competencia empresarial, los ladrones de identidad o individuos sin escrúpulos la ven, la capturan y la explotan. Hasta una persona curiosa casual puede ser una amenaza potencial. Desde contraseñas a números de cuenta, datos financieros e información propietaria de la empresa, todo está en riesgo, y ninguna cantidad de seguridad de software puede evitar que estos fisgones de datos echen un vistazo.

Mientras que el lugar de trabajo actual sigue expandiéndose fuera de las oficinas tradicionales, a espacios remotos y públicos, la posibilidad de ser atacado por un "hacker visual" es más real que nunca. De hecho, la piratería visual es la amenaza de baja tecnología más subestimada a la que se enfrentan las empresas hoy en día. Es sencilla, efectiva y pasa desapercibida hasta que es demasiado tarde.

Según una investigación publicada por el Ponemon Institute[1]:

- El 91 % de los intentos de piratería visual tuvieron éxito
- El 68 % de los intentos de piratería visual pasaron desapercibidos para la víctima
- El 52 % de la información confidencial se capturó directamente de las pantallas del dispositivo

Manténgase al tanto de su entorno.

Al trabajar en espacios públicos, asuma siempre que alguien podría mirar por encima de su hombro y elija las tareas en consecuencia.

Limite su exposición.

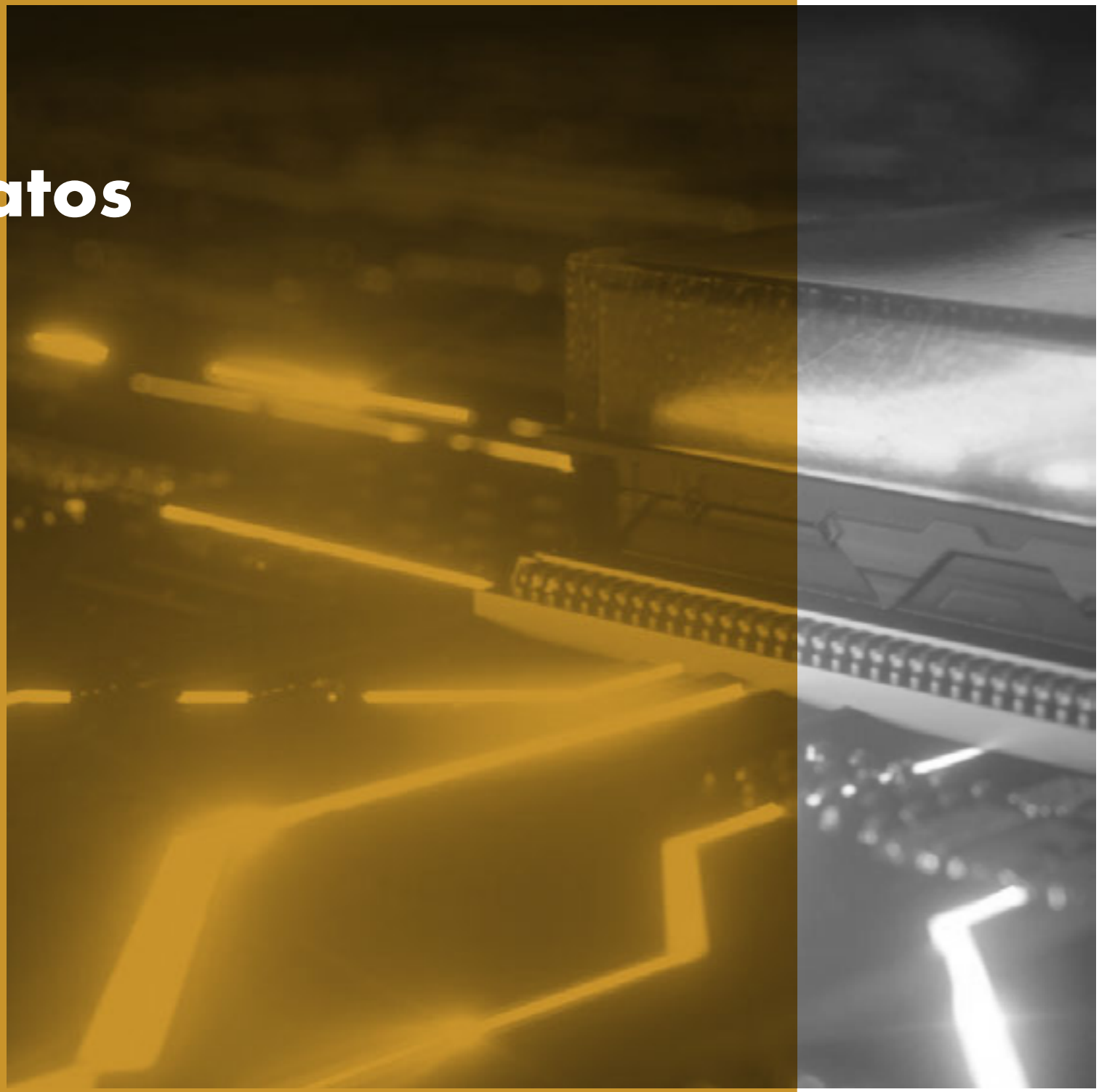
Las pantallas privadas están diseñadas para reducir los ángulos de visión de la pantalla, para que un hacker potencial no pueda ver lo que se muestra en la pantalla si no está directamente en frente. Un filtro externo es una manera sencilla de añadir seguridad. Se acopla sobre la pantalla y se puede eliminar cuando necesite compartir la pantalla con más gente.

De manera alternativa, una pantalla privada integrada simplifica este proceso, y al mismo tiempo elimina la necesidad de aplicar, guardar y reemplazar un protector externo. Muchos ordenadores de HP ofrecen como opción, HP Sure View Gen2[15], una pantalla privada integrada diseñada para evitar la piratería visual. Funciona modificando dinámicamente la estructura de los píxels LCD a nivel molecular, permitiendo que se habilite o deshabilite con un botón y mejorando el rendimiento tanto en entornos luminosos como oscuros.

15—La pantalla privada integrada de HP Sure View es una función opcional que se debe configurar con la compra y que está diseñada para funcionar con la orientación horizontal.

Sección 9:

Cifre sus datos



Cuando se pierde o se roba un PC, el disco duro es el primer punto de ataque. Lo sujetan solo un par de tornillos y, una vez que se saque, se puede colocar en otro PC. Si no ha protegido sus datos correctamente, leer un disco es tan fácil como leer un libro.

El cifrado asegura que todos los datos sigan siendo completamente inteligibles. El cifrado es un proceso para codificar los datos y hacerlos ilegibles para cualquier persona que no tenga la clave secreta de descodificación. Así que un ordenador con un disco duro cifrado puede ser robado pero no se puede acceder a la información: un resultado mucho mejor que su información personal o empresarial acabe en las manos equivocadas para siempre.

Permita el cifrado de software.

Windows 10 Pro es compatible con el cifrado de contraseñas de su disco duro, usando sus credenciales de inicio de sesión como clave. Esto asegura que un hacker necesitaría su nombre de usuario y contraseña para acceder a sus datos.

Asegúrese de que tiene una contraseña segura para su cuenta de usuario:

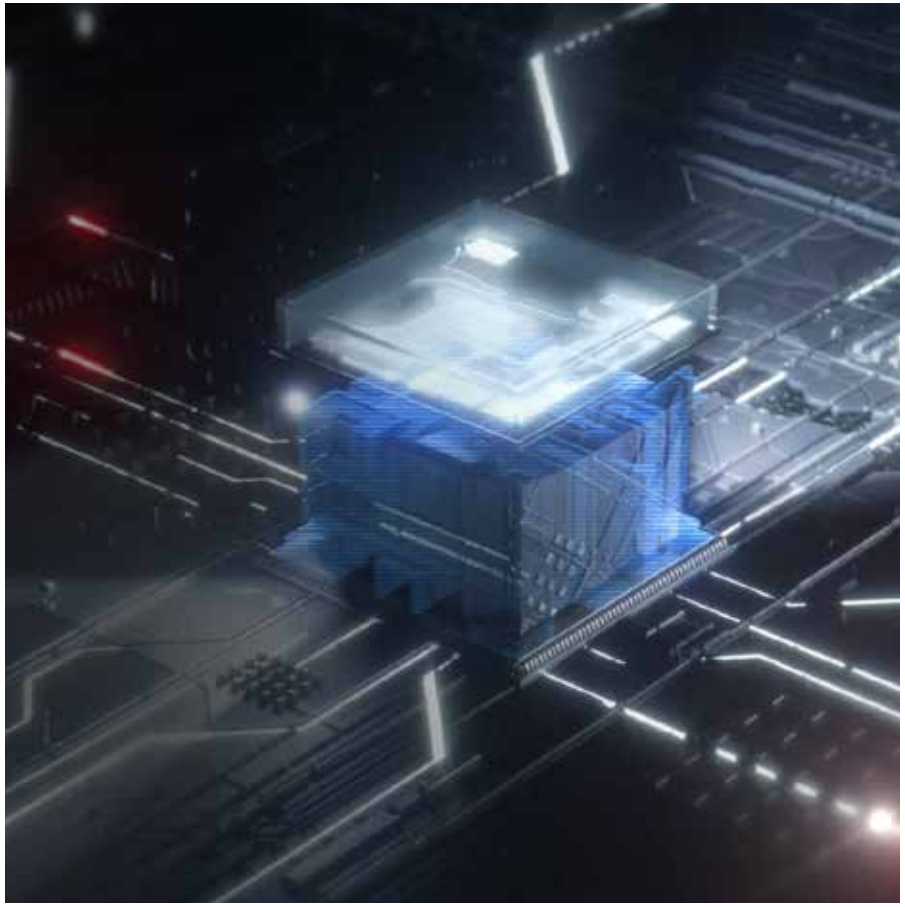
1.
   - Ajustes > Cuentas > Opciones de inicio de sesión> Contraseña

2. Si está disponible, habilite el Gestor de Plataforma de Confianza (TPM, por sus siglas en ingles), que activa un chip de seguridad en su PC para cifrar sus contraseñas nuevas y sus datos en el disco:
   - Configuración> Actualización y seguridad> Seguridad de Windows> Seguridad del dispositivo> Procesador

3. Active el cifrado, asegurando que sus datos no podrán ser vistos o copiados sin sus credenciales:
   - Configuración> Actualización y seguridad> Cifrado de disco

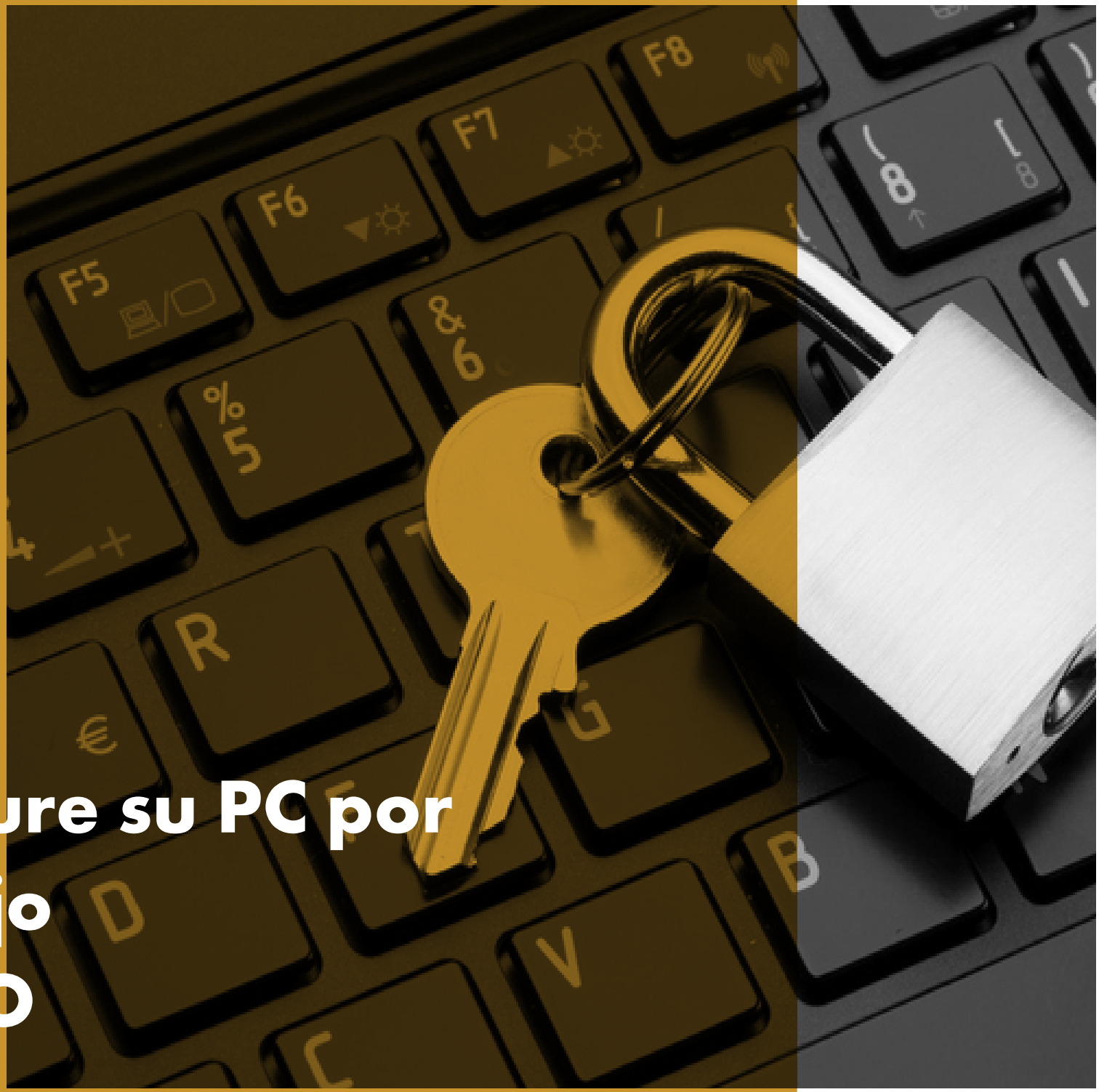
Benefíciese del cifrado de hardware.

BitLocker es una función de Windows 10 Pro que proporciona cifrado de software que se desbloquea con una clave de hardware. Los dispositivos que tienen un chip TPM, como los portátiles HP, pueden cifrar sin el hardware extra. TPM evita el acceso a datos cifrados si detecta que el sistema ha sido manipulado cuando estaba apagado. Los dispositivos sin TPM también pueden usar BitLocker, pero necesitarán un dispositivo extraíble, como un USB, como clave.



Sección 10:

Asegure su PC por debajo del SO



BIOS (Basic Input Output Software) es un software que inicia el ordenador y le ayuda a cargar el sistema operativo. Al infectar este software central, los espías pueden colocar malware que se mantenga vivo y sin detectar por el antivirus. Se queda ahí incluso si se elimina el disco duro o si se reinstala el sistema operativo.

Si un hacker consigue acceder a su BIOS, básicamente se apropiará de todos los aspectos de su PC.

Esto le da al atacante una manera de filtrar los datos y bloquear el sistema modificando el firmware, lo que requeriría reemplazar toda la placa del sistema para repararlo.
Para HP Elite y ordenadores Pro, HP Sure Start puede reparar automáticamente la BIOS de malware, rootkits o corrupciones, añadiendo una capa extra de protección y creando una base de confianza para la seguridad de su PC[16].

No ignore ninguna actualización.

Como mencionamos anteriormente en la sección 4, las actualizaciones de software aseguran que se apliquen parches a las nuevas vulnerabilidades, y la BIOS no es una excepción. Como la mayoría de implementaciones BIOS comparten el mismo código fuente a través de toda la fuerza de trabajo o base de usuarios, es posible que cualquier vulnerabilidad descubierta esté presente en muchas implementaciones a través del entorno del proveedor de PC. Las herramientas OEM como HP Support Assistant buscan actualizaciones automáticamente, o puede comprobar el sitio del fabricante para buscar actualizaciones de BIOS.

Ahonde en la BIOS.

La configuración de fabrica de la BIOS se puede ver como un equilibrio entre seguridad y usabilidad. Sin embargo, para proteger al sistema contra los muchos posibles métodos de transferir código malicioso, puede que deba eliminar algunas de las funcionalidades.

El acceso a la configuración de la BIOS puede variar de un fabricante a otro, pero normalmente hay que presionar una tecla funcional durante el arranque inicial (F10 o FN-10 para los portátiles HP).

16—HP Sure Start Gen4 está disponible en los productos HP Elite y HP Pro 600 equipados con procesadores Intel® o AMD de 8.ª generación.

Establezca una contraseña BIOS.

Para proteger la configuración BIOS ante un posible cambio por parte de un usuario no autorizado, se recomienda establecer una contraseña BIOS:

- Por ejemplo: Seguridad> Herramientas de administrador> Crear contraseña de administrador para BIOS

Es importante recordar la contraseña BIOS, ya que está diseñada para que no se pueda sortear ni recuperar.

Establezca una contraseña de inicio.

Para una mayor seguridad, se puede crear una contraseña de inicio. Cada vez que se enciende el PC, antes de que el sistema ejecute nada, se pide la contraseña de inicio. Como la contraseña BIOS, tampoco puede recuperarse ni restablecerse fácilmente, y olvidarla hace que la máquina sea inutilizable.

Limite las funciones sin usar.

En la BIOS, hay que considerar unos cuantos ajustes para una seguridad máxima. Aunque pueden eliminar ciertas funciones o reducir la accesibilidad, la seguridad por debajo del SO que facilitan no se puede replicar igualmente con el software:

1. Elimine dispositivos externos y ópticos de la orden de arranque (p. ej., Avanzadas> Opciones de arranque). Sobre todo el arranque de almacenamiento de USB, el arranque de red (PXW) y el arranque de disco óptico, ya que estos permiten que se cargue malware de fuentes externas. Si es necesario el arranque desde estos dispositivos, se puede habilitar la función caso por caso.

2. Deshabilite el soporte heredado (p. ej., Avanzadas> Configuración de arranque seguro) y habilite el arranque seguro.

3. Active la función “Almacenamiento/restauración GPT del disco duro del sistema” (p. ej., Seguridad> Funciones del disco duro).

4. Habilite DriveLock y establezca una contraseña.

Conclusión

En la actualidad, cada vez más amenazas digitales se dirigen a pequeñas y medianas empresas. La buena noticia es que la mayoría del hardware y software que tiene incluye funciones de seguridad desaprovechadas que le pueden ayudar a combatirlas. También hay un número sin precedentes de productos y servicios disponibles con innovaciones de seguridad punteras para protegerle contra el futuro desconocido. Desde seguridad basada en hardware hasta dispositivos contemporáneos para actualizar software, una pequeña inversión en dispositivos conectados y seguros le será rentable a la larga. HP diseña soluciones de seguridad que sacan el máximo rendimiento a los puntos fuertes de Windows 10 Pro, apoyando las funciones de seguridad integradas con mejoras de hardware discretas y soporte de software siempre actualizado. Las amenazas a las que se enfrenta evolucionan a diario y una estrategia de seguridad mejorará sustancialmente las posibilidades de ganar.

GRACIAS.

Si desea obtener más información, visite:
www.hp.com/go/windows10now

+ Windows 10

Protéjase desde el encendido al apagado.