Guía de Implementaciones de controles de ciberseguridad para PYMEs

A continuación, se presentan algunas posibles opciones de implementación de los controles de la guía de controles de ciberseguridad, simples, prácticas y de bajo costo para la protección integral de la PYME.

Archivos (en computadoras, teléfonos, dispositivos móviles, etc.)

1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos:

La implementación de este control fue planteada como un control de equipos (computadoras, teléfonos y dispositivos móviles). Ver sección "Computadoras", Control 1.

2. Cifrado de archivos sensibles:

Cifrado de archivos en computadoras:

Opción 1:

AxCrypt permite cifrar archivos de manera simple e integrada al menú contextual del explorador de archivos de Windows (también disponible para iOS). Se debe hacer click derecho sobre el archivo que quiere cifrar y elegir la opción de cifrar. Se puede cifrar carpetas enteras. Posee un gestor de contraseñas integrado (opcional), de manera a que el usuario no necesite ingresar la contraseña cada vez que quiere abrir el archivo.

Tipo de control: Herramienta a nivel de equipo

Herramientas: AxCrypt

Tiempo estimado: 2 a 3 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlaces: https://www.axcrypt.net/es/download/

Opción 2:

La función de Password Protection de Microsoft Office permite cifrar documentos de texto, planillas electrónicas y presentaciones, ya viene incluido con la suite ofimática. Para cifrar archivos de otros formatos (pdf, imágenes, etc.) se puede utilizar 7zip para crear un archivo comprimido (.rar, .zip o similar) con contraseña.

Tipo de control: Herramienta a nivel de equipo

Herramientas: 7zip

Tiempo estimado: 2 a 3 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlaces:

https://support.office.com/en-us/article/Add-or-remove-protection-in-your-document-workbook-or-presentation-05084cc3-300d-4c1a-8416-38d3e37d6826

https://basicoyfacil.wordpress.com/2012/03/11/proteger-con-contrasena-un-archivo/

Opción 3:

Veracrypt es una herramienta que crea un contenedor virtual cifrado. Todos los archivos que se almacenan en dicho contenedor estarán protegidos

Tipo de control: Herramienta a nivel de equipo

Herramientas: Software Veracrypt

Tiempo estimado: 30 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: nivel intermedio

Costo: ninguno

Enlaces: https://www.veracrypt.fr/en/Home.html

Tutorial de uso incluido en la herramienta.

Cifrado de archivos en Teléfonos o dispositivos móviles:

Los teléfonos Android y iOS ya traen una funcionalidad de cifrado de archivos a nivel de disco (full-disk encryption). En algunos modelos, viene activo por defecto; se utiliza el PIN, patrón o huella de desbloqueo para el cifrado y descifrado.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 2 minutos por equipo

Personal necesario: cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlaces:

https://docs.microsoft.com/es-es/intune-user-help/encrypt-your-device-android

https://ssd.eff.org/es/module/c%C3%B3mo-encriptar-su-iphone

3. Distribución granular de permisos para accesos a archivos:

La organización debe realizar un inventario de activos de información, en la que, como mínimo, se debe recoger la siguiente información:

- ¿Qué tipo de datos o información poseemos en la empresa?
- De estos datos, ¿cuáles son sensibles?
- ¿Dónde están almacenados esos datos, en qué archivos, en qué máquinas, en qué cuentas?
- ¿Quiénes tienen acceso a esos datos actualmente?
- ¿Quiénes necesitan esos datos para realizar sus tareas?

Luego de haber respondido dichas preguntas, debe tomar las decisiones necesarias para definir los niveles de permiso de acuerdo a cada empleado o grupo de empleados. Por último, habiendo definido quién va a tener acceso a qué, debe asegurarse de eliminar y/o restringir el acceso a cualquier archivo o activo de información por parte del personal que no ha quedado autorizado.

Tipo de control: Procedimiento de la organización

Herramientas: Formulario de inventario de información

Tiempo estimado: 4 a 30 horas

Personal necesario: 1 persona completa y apoyo de un directivo o autoridad de la empresa, como mínimo; adicionalmente, apoyo de los demás empleados.

Conocimiento técnico: ninguno

Costo: ninguno

4. Copia de seguridad continua de archivos:

Opción 1:

OneDrive for Business permite la sincronización de archivos en la nube de OneDrive de Microsoft, mediante una cuenta corporativa. En caso de que cuente con una suscripción, desde la más básica, el servicio ya está incluido, con un almacenamiento de 1TB, solo debe instalarse el software cliente en las máquinas que se deseen sincronizar. En caso de que la empresa no posea una suscripción y no desee pagar suscripciones, cualquier empleado que posea una cuenta de Microsoft o Outlook puede usar la versión personal de OneDrive (5GB de almacenamiento).

Tipo de control: Funcionalidad incluida en servicio - suscripción

Herramientas: software para OneDrive for Business

Tiempo estimado: 5 a 10 minutos por equipo (adquisición y configuración del servicio OneDrive for Business 30 minutos a 1 hora)

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno – Obs.: incluido con la suscripción básica de OneDrive for Business, 5 dolares al mes por usuario; alternativa gratuita: OneDrive Personal, incluido con el servicio gratuito de cuenta personal de Microsoft o de Outlook.

Enlaces: https://support.office.com/en-us/article/Set-up-your-computer-to-sync-your-OneDrive-for-Business-files-in-Office-365-23e1f12b-d896-4cb1-a238-f91d19827a16

Opción 2:

Zoho Docs es un servicio corporativo que ofrece, entre otras cosas, la sincronización de archivos en la nube de Zoho, mediante una cuenta corporativa. Posee un plan gratuito para 25 usuarios (ampliable hasta 50 a través del programa de Referrers), con un almacenamiento de 5GB por usuario, solo debe instalarse el software cliente en las máquinas que se deseen sincronizar.

Tipo de control: Funcionalidad incluida en servicio - suscripción

Herramientas: software cliente para Zoho Docs

Tiempo estimado: 5 a 10 minutos por equipo (adquisición y/o configuración del servicio Zoho 30 minutos a 1 hora)

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno hasta 25 usuarios (ampliable a 50 mediante Referrers)

Enlace: https://www.zoho.com/docs/desktop-sync.html

Computadoras:

1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos:

Opción 1:

El establecimiento de contraseña de inicio de sesión y pantalla de bloqueo con contraseña en Windows con forzado de cumplimiento de política a través de la edición manual de Local Security Policy permitirá que la empresa se asegure que los empleados están cumpliendo con la política de contraseña para el acceso al equipo.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 15 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://technet.microsoft.com/en-us/library/dd277399.aspx?f=255&MSPPError=-2147217396

Opción 2:

El establecimiento de contraseña de inicio de sesión y pantalla de bloqueo con contraseña en Windows con forzado de cumplimiento de política a través de la importación de un *template* securizado con la herramienta LGPO y Security Compliance Manager (SCM) permitirá que la empresa se asegure que los empleados están cumpliendo con la política de contraseña para el acceso al equipo. Tiene la ventaja que no se necesita modificar la política de manera manual en cada equipo, sino se puede simplemente editarla de acuerdo a las necesidades en un equipo (por defecto, el *template* ya está securizado para cumplir con los requerimientos comunes) y luego puede importarse en las demás máquinas con la herramienta LGPO.

Podría generar problemas si el *template* restringe alguna funcionalidad que la empresa necesita, en cuyo caso el *template* debe ser modificado previamente, lo cual requiere un nivel de conocimiento intermedio/avanzado. La ventaja es que el *template* ofrece no solo hardening de políticas de contraseña sino muchas otras configuraciones seguras, que se aplicarán en pocos minutos.

Tipo de control: Herramienta a nivel de equipo

Herramientas: LGPO y Security Compliance Manager (SCM)

Tiempo estimado: 30 minutos a 1 hora para la personalización del *template* (opcional) y 2 a 3 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos

Conocimiento técnico: intermedio

Costo: ninguno

Enlaces:

https://technet.microsoft.com/es-es/solutionaccelerators/cc835245.aspx

https://blogs.technet.microsoft.com/secguide/2016/09/23/lgpo-exe-v2-0-pre-release-support-for-mlgpo-and-reg_qword/

Tutorial de uso incluido en la herramienta.

En ambas opciones se requiere que, luego de aplicar la política, los usuarios existentes cambien sus contraseñas, ya que las políticas se aplican a contraseñas nuevas, no a los existentes.

2. Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.)

Opción 1:

Tipo de control: Herramienta a nivel de equipo

Herramientas: antivirus Kaspersky Free

Tiempo estimado: 30 a 45 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://www.kaspersky.com/downloads/thank-you/free-antivirus-download

Opción 2:

Tipo de control: Herramienta a nivel de equipo

Herramientas: antivirus AVAST

Tiempo estimado: 20 a 30 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://www.avast.com/es-ww/index

Opción 3:

Windows Defender viene incluido a partir de Windows 10, se active la función desde el panel de control.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por equipo

Personal necesario: 1 persona para la activación en todos los equipos o cada empleado lo activa individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://www.microsoft.com/es-es/windows/comprehensive-security

Opción 4:

Existen soluciones corporativas para PYMEs que incluyen funcionalidades adicionales a las gratuitas, entre ellas la más importante, acceso a una consola de administración central, como por ejemplo AVAST Business Managed Antivirus

Tipo de control: Herramienta a nivel de equipo + servicio Cloud

Herramientas: antivirus AVAST Business Managed Antivirus

Tiempo estimado: 1 a 2 horas para la configuración de la consola central + 15 a 25 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o 1 persona para la configuración de la consola central y cada empleado instala individualmente el software antivirus.

Conocimiento técnico intermedio

Costo: planes anuales (1, 2 o 3 años), 20 a 40 USD por equipo por año; precio unitario inversamente proporcional a la cantidad de equipos y tiempo de licencia.

Enlace: https://www.avast.com/lp-managed-antivirus?quantity=8&id=BMS-00

3. Firewall basado en Host

Opción 1:

Windows incluye un firewall personal, normalmente se encuentra activo por defecto

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://support.microsoft.com/es-es/help/4028544/windows-turn-windows-firewall-on-or-off

Opción 2:

Algunas herramientas de antivirus como Baidu u FortiClient incluyen la funcionalidad de firewall. En otros antivirus, es una funcionalidad de pago.

Tipo de control: Herramienta de nivel de equipo

Herramientas: antivirus (por ejemplo, FortiClient u otro que incluya firewall)

Tiempo estimado: 1 a 2 minutos por equipo (se considera que la herramienta de antivirus ya se encuentra instalada y configurada)

Personal necesario: 1 persona para la activación en todos los equipos o cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlaces:

http://antivirus.baidu.com/en/

https://www.forticlient.com/downloads

4. Actualización de sistema operativo y programas:

Opción 1:

La gran mayoría de sistemas operativos, entre ellos Windows, iOS y Linux permiten la actualización automática.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por equipo

Personal necesario: 1 persona para la configuración en todos los equipos o cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlaces:

https://support.microsoft.com/es-es/help/12373/windows-update-faq

https://support.apple.com/en-us/HT201541

Opción 2:

Muchas aplicaciones incluyen la funcionalidad de verificación de versión y actualización automática en la propia aplicación. Asegúrese que sus aplicaciones, en caso de permitirlo, tengan activada la opción de comprobación automática de actualización.

Opción 3:

Kaspersky Software Updater es una herramienta de gestión de actualizaciones que realizan un análisis de qué aplicaciones están instaladas en el equipo, verifican si existe una versión posterior y, en caso de comprobar que se encuentra desactualizado, notifica al usuario o administrador.

Tipo de control: Herramienta de nivel de equipo

Herramientas: Kaspersky Software Updater

Tiempo estimado: 30 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://latam.kaspersky.com/free-software-updater

Opción 4:

En caso de que cuente con un dominio, Microsoft ofrece una herramienta para gestión centralizada de actualizaciones en redes corporativas llamada Microsoft Windows Server Update Services (WSUS), incluida como un rol desde Windows Server 2008 R2, sin ningún costo adicional. WSUS, al igual que Microsoft Update, gestiona las actualizaciones de productos de Microsoft, sin embargo, puede ser combinada con otro software de gestión de actualizaciones complementarios, como por ejemplo Local Update Publisher.

Tipo de control: Herramienta de nivel de equipo y funcionalidad de sistema operativo (servidor)

Herramientas: Local Update Publisher y WSUS

Tiempo estimado: 8 a 24 horas (se asume que ya se cuenta con un servidor Windows Server 2008 R2 o superior instalado y configurado de manera funcional)

Personal necesario: 1 persona

Conocimiento técnico: avanzado

Costo: ninguno (se asume que ya se ha adquirido una licencia válida de Windows Server)

Enlaces:

https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services

http://localupdatepubl.sourceforge.net/

5. Protección de servicios expuestos con contraseñas robustas:

Algunos de los principales servicios de acceso remoto que pueden ser expuestos a Internet son SSH, RDP, TeamViewer. En el caso de RDP, se aplican las políticas de contraseñas del equipo o del dominio, ver control 1 de la presente sección. En el caso de otros mecanismos, como SSH, se debe establecer la política mediante el cambio de configuración del servicio.

Opción 1:

Configuración de políticas de contraseña del servicio SSH.

Tipo de control: Funcionalidad del servicio

Herramientas: ninguna

Tiempo estimado: 15 minutos por equipo

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno

Enlace: https://linux-audit.com/audit-and-harden-your-ssh-configuration/

Teléfonos y dispositivos móviles

1. Antivirus:
   - ESET Mobile Security & Antivirus
   - AVG Antivirus
   - AVAST Antivirus
   - Antivirus Free-Mobile Security (NQ Security Lab)
   - Antivirus Kaspersky para móviles y tablets

Tipo de control: Herramienta de nivel de equipo

Herramientas: diversas aplicaciones de los *app stores* oficiales

Tiempo estimado: 1 a 3 minutos

Personal necesario: 1 persona para la instalación en todos los dispositivos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

2. Restricción de instalación de apps no oficiales:

Tanto Android como iOS permiten restringir la instalación de aplicaciones que no provengan de los *app stores* oficiales, mediante una configuración del sistema operativo.

Tipo de control: Configuración a nivel del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona para la configuración de todos los dispositivos o cada empleado lo configura individualmente. Obs.: Por defecto, ya viene configurado de esta manera, por lo que, a menos que alguien lo hubiera cambiado manualmente, no sería necesario realizar ninguna acción adicional, más que verificar que está configurado de esta manera.

Conocimiento técnico: ninguno

Costo: ninguno

3. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña

Andoid y iOS permiten establecer una contraseña, un PIN numérico, un patrón de desbloqueo o algún rasgo biométrico (huella dactilar, imagen facial, u otro). A diferencia de las computadoras, no suele ser posible establecer una política de robustez de dicha credencial, las opciones específicas dependen del fabricante del dispositivo (modelo, marca, etc.). Por defecto no viene configurado ninguna contraseña ni equivalente.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por equipo

Personal necesario: Cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Correo electrónico

1. Contraseña segura:

Opción 1:

En caso de que cada empleado utilice su cuenta personal de Gmail, Hotmail u otro similar, la empresa solo puede instruir a cada empleado a que utilice una contraseña robusta, pero dependerá de cada empleado de obedecer ese requerimiento.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: Cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

En caso de que utilizar un servicio de correo corporativo como Zoho Mail es posible establecer una política de contraseña a través del panel de administración, de modo a asegurar que todos los empleados estén utilizando contraseñas robustas en las cuentas de correo electrónico.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

Enlace:

https://www.zoho.com/mail/help/adminconsole/password-policy.html

2. Autenticación de doble factor:

Opción 1:

En caso de que cada empleado utilice su cuenta personal de Gmail, Hotmail u otro similar, las cuales incluyen la funcionalidad de autenticación de doble factor, la empresa debe instruir a cada empleado a que la active y configure.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: depende del servicio (por ej., Google Authenticator)

Tiempo estimado: 10 a 15 minutos por cuenta

Personal necesario: Cada empleado lo configura individualmente.

Conocimiento técnico: básico

Costo: ninguno

Enlace:

https://support.google.com/accounts/answer/185839?hl=es-419

https://support.microsoft.com/es-py/help/4028586/microsoft-account-turning-two-step-verification-on-or-off-for-your-mic

https://www.cert.gov.py/application/files/8914/3230/6320/Autenticacion_Doble_Factor.pdf

Opción 2:

En caso de que utilizar un servicio de correo corporativo como Zoho Mail es posible activar y forzar el uso de autenticación de doble factor a través del panel de administración, de modo a asegurar que todos los empleados sean forzados a configurarla en su cuenta.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: teléfono móvil, cuenta de correo alternativa o Google Authenticator

Tiempo estimado: 1 a 2 minutos para la activación desde el panel de administración, 10 a 15 minutos por cuenta

Personal necesario: 1 persona para la activación y cada empleado lo configura individualmente para su cuenta.

Conocimiento técnico: básico

Costo: ninguno

Enlace: https://www.zoho.com/mail/help/adminconsole/two-factor-authentication.html

3. Configuración segura del servidor de correo, restricción del puerto 25:

Para implementar este control, se debe incluir las siguientes reglas en el cortafuego a nivel de red:

- Restringir el tráfico desde y hacia la LAN por puerto 25
- Permitir el tráfico desde la IP del servidor de correo hacia la WAN por puerto 25

Una PYME puede implementar esta restricción en el equipo de borde de red (router) o en un sistema dedicado (físico o virtual). En el caso de redes que no cuentan con IPs públicas estáticas, la gran mayoría de los proveedores de servicio de internet nacionales restringen el tráfico desde y hacia el puerto 25.

Tipo de control: Funcionalidad del equipo de red

Herramientas: ninguna

Tiempo estimado: 3 a 5 minutos

Personal necesario: 1 persona

Conocimiento técnico: intermedio a avanzado

Costo: ninguno

Enlace: http://www.tp-link.com/ar/faq-158.html

4. Actualización del software de correo (si es propio):

Si la empresa cuenta con un servidor de correo propio, deberá actualizar regularmente el software de correo. Esto deberá ser llevado a cabo por el administrador del servicio de correo, las instrucciones específicas dependerán del software de correo a ser utilizado.

Opción 1:

En caso de que utilizar por ejemplo Zimbra, la instalación de parches de seguridad, en una misma versión, se realiza desde la consola del servidor. En caso de que se trate de una versión nueva, se debe hacer una migración de versión, también desde la consola.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 15 minutos a 8 horas (dependiendo de si la actualización es de una nueva versión)

Personal necesario: 1 persona

Conocimiento técnico: intermedio - avanzado

Costo: ninguno

Enlace: https://wiki.zimbra.com/wiki/Zimbra_Releases/8.7.0/Upgrade

5. Configuración de información de recuperación:

La gran mayoría de los servicios de correo permiten establecer información de recuperación tal como una cuenta de correo alternativa, un número de teléfono móvil, etc. La implementación específica depende del tipo de servicio de correo utilizado.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: cada empleado lo configura individualmente para su cuenta.

Conocimiento técnico: básico

Costo: ninguno

Redes Sociales:

1. Contraseña segura:

La implementación específica de esta medida de protección depende de cada red social. En la mayoría de los casos, las redes sociales se manejan como cualquier cuenta personal y la empresa solo puede instruir a los administradores de la red social a que utilices una contraseña robusta, pero dependerá de éstos obedecer ese requerimiento.

Tipo de control: Funcionalidad de la plataforma de red social

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: Cada empleado que administra una cuenta lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

2. Autenticación de doble factor:

Al igual que en el correo electrónico, la implementación de esta medida de protección depende, en gran medida, de cada plataforma de red social (Facebook, Twitter, Instagram, etc.). La gran mayoría de estas plataformas incluyen la funcionalidad de autenticación de doble factor, la cual simplemente debe ser activada y configurada por los usuarios.

Tipo de control: Funcionalidad del servicio de red social

Herramientas: teléfono móvil, cuenta de correo alternativa o Google Authenticator

Tiempo estimado: 10 a 15 minutos por cuenta por plataforma

Personal necesario: cada empleado que administra una cuenta lo configura individualmente para la cuenta.

Conocimiento técnico: básico

Costo: ninguno

Enlaces:

https://www.facebook.com/help/148233965247823?helpref=faq_content

https://help.twitter.com/es/managing-your-account/two-factor-authentication

https://www.facebook.com/help/instagram/566810106808145

3. Configuración de información de recuperación:

La implementación específica depende de la red social utilizada, pero la gran mayoría (Facebook, Twitter, Instagram) lo permite. Muchas veces, el número telefónico configurado para la autenticación de doble factor constituye la información de recuperación.

Tipo de control: Funcionalidad de la red social

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta por plataforma

Personal necesario: cada empleado que administra una cuenta lo configura individualmente para la cuenta.

Conocimiento técnico: ninguno

Costo: ninguno

4. Procedimiento de baja de usuario - transferencia de responsabilidades y accesos:

Existen diversas maneras de implementar este control, dependiendo de la plataforma y de la empresa, ya sea a través de la redundancia de roles (más de un usuario administrador, cuando la plataforma lo permite), resguardo de la contraseña en poder de una autoridad de la empresa, u otros mecanismos por lo que no se ha probado la implementación, sin embargo, puede realizarse sin conocimientos técnicos y sin costo económico.

Wifi:

1. Contraseña segura del Wifi:

La contraseña del wifi se establece a través del panel de administración del Access Point (AP). Las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos. La contraseña debe cumplir las políticas de contraseña de la empresa especialmente en cuanto a longitud y complejidad.

Tipo de control: Configuración a nivel de equipo (AP)

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona

Conocimiento técnico: ninguno

Costo: ninguno

Enlaces: https://es.wikihow.com/cambiar-la-contrase%C3%B1a-de-WiFi

2. Configuración segura del Wifi – protocolos seguros:

La configuración se realiza a través del panel de administración del Access Point (AP), las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos. Para una PYME, el protocolo más adecuado es WPA2; nunca se debe utilizar WEP o WPA.

Tipo de control: Configuración a nivel de equipo (AP)

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://es.wikihow.com/cambiar-la-contrase%C3%B1a-de-WiFi

3. Contraseña segura del Access Point:

La contraseña del AP se establece a través del panel de administración del AP. Las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos.

Tipo de control: Configuración a nivel de equipo (AP)

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: http://www.tp-link.com/ve/faq-73.html

4. Utilización de HTTPs para envío de credenciales:

Opción 1:

Puede utilizar HTTPS Everywhere, un complemento para navegadores que fuerza el uso de HTTPs durante la navegación.

Tipo de control: Herramienta de nivel de equipo

Herramientas: HTTPS Everywhere

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://www.eff.org/https-everywhere

Página Web:

1. Actualización de CMS, plugins, plantillas:

La gran mayoría de los CMS, plugins y plantillas pueden actualizarse a través del panel de administración del CMS, sin embargo, las instrucciones específicas pueden variar de acuerdo al CMS, al plugin y a la plantilla. Por ejemplo, existen plugins que deben ser actualizados reemplazando los archivos a través del FileManager o FTP. Algunos proveedores de servicio de alojamiento ofrecen la funcionalidad de actualización automática de los componentes. Para una PYME que no cuenta con personal técnico, es preferible elegir un servicio de hosting que cuente con esta funcionalidad.

Tipo de control: Funcionalidad del hosting o procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 5 a 30 minutos, dependiendo del CMS, plugin o plantilla

Personal necesario: 1 persona

Conocimiento técnico: básico a intermedio

Costo: ninguno

Enlaces:

https://www.sitepoint.com/a-guide-to-updating-wordpress/

https://www.webempresa.com/blog/actualizar-plugins-temas-wordpress.html

https://docs.joomla.org/J3.x:Updating_from_an_existing_version/es

2. Contraseña segura para los usuarios del CMS:

Tipo de control: Funcionalidad del CMS

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por cuenta

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

3. Auditoría de vulnerabilidades de la aplicación web (en caso de desarrollo propio):

Opción 1:

Un análisis de vulnerabilidades básico de una web puede ser realizado con scanners gratuitos como ZAP.

Tipo de control: Herramienta y procedimiento de la empresa

Herramientas: ZAP Scanner

Tiempo estimado: 15 a 30 minutos para análisis

Personal necesario: 1 persona

Conocimiento técnico: avanzado

Costo: ninguno

Enlace:

http://www.toobler.com/blog/zap-penetration-testing-simple-tutorial

https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerabilities-for-any-website-using-nikto-0151729/

Opción 2:

Se puede contratar un servicio de análisis de vulnerabilidades básico, pudiendo incluir o no la corrección de vulnerabilidades encontradas. En las PYMEs, raramente habrá los recursos para corregir las vulnerabilidades, por lo que el servicio debe incluirlo, o se debe contratar otro servicio para ello.

Tipo de control: Servicio tercerizado

Herramientas: No aplica

Tiempo estimado: No aplica

Personal necesario: 1 persona para acompañamiento del proceso

Conocimiento técnico: básico a intermedio

Costo: 500 a 1000 Euros

4. Contraseña segura para accesos del hosting:

Tipo de control: Funcionalidad del hosting

Herramientas: ninguna

Tiempo estimado: 3 a 5 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

5. Copia de seguridad del sitio web:

Opción 1:

Se puede hacer una copia manualmente, copiando el contenido del sistema de archivos, del directorio raíz del servidor web, y el contenido de la base de datos. Se puede comprimir todo el contenido o crear un archivador con los archivos y se debe guardar offline, preferentemente, ya sea en un dispositivo de almacenamiento (USB, disco duro externo o similar) u online, pero fuera del servidor web.

Tipo de control: Procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 5 a 15 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

Opción 2:

Algunos servicios de alojamiento ofrecen la funcionalidad de copia de seguridad automática, solo se debe indicar la frecuencia con la que se desea realizar la copia, la cantidad de copias que se desea almacenar, el lugar donde se desea almacenar, etc. La mayoría de las veces, solo se permite guardar localmente en el mismo servicio de hosting, lo cual podría constituir un riesgo en caso de que el incidente se da con el servicio de hosting justamente. En caso de que el servicio no permita configurar un almacenamiento externo, el administrador deberá descargar regularmente la copia de seguridad de manera manual.

Tipo de control: Funcionalidad del servicio de alojamiento + procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

6. Separación de bases de datos y/o archivos sensibles del contenedor público:

En caso de que la empresa cuente con bases de datos sensibles, ésta debe estar en un servidor de bases de datos distinta al de la página web. El administrador del servidor web debe realizar una revisión para asegurar que esto se esté cumpliendo, en caso contrario, debe migrar el contenido sensible a otro servidor; un servidor virtual o un contenedor virtual distinto será adecuado.

Tipo de control: Procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 10 a 60 minutos

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno

Enlace: https://blog.desdelinux.net/manten-la-seguridad-de-tus-bases-de-datos-mysql-creando-usuarios-y-permisos-separados/

Servicios en la nube:

1. Contraseña segura:

Opción 1:

Si se trata de un servicio en la nube orientado a uso personal, la empresa debe dar la directiva a los usuarios que administran la cuenta del servicio para que éstos establezcan una contraseña segura.

Tipo de control: Funcionalidad de la plataforma

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: Cada empleado que administra una cuenta lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

Si se trata de un servicio en la nube orientado a uso corporativo, el administrador del servicio debe configurar la política de contraseña a través del panel de administración de la nube. La implementación de este control dependerá de la plataforma.

Tipo de control: Funcionalidad de la plataforma

Herramientas: ninguna

Tiempo estimado: 5 minutos por plataforma

Personal necesario: 1 persona.

Conocimiento técnico: ninguno

Costo: ninguno

2. Autenticación de doble factor:

Opción 1:

Si se trata de un servicio en la nube orientado a uso personal, la empresa debe dar la directiva a los usuarios que administran la cuenta del servicio activen y configuren la autenticación de doble factor a la cuenta asociada al servicio.

Tipo de control: Funcionalidad de la plataforma

Herramientas: depende de la plataforma (teléfono, Google Authenticator, etc.)

Tiempo estimado: 10 a 15 minutos por cuenta

Personal necesario: Cada empleado que administra una cuenta lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://www.dropbox.com/es_ES/help/security/enable-two-step-verification

Opción 2:

Si se trata de un servicio en la nube orientado a uso corporativo, el administrador del servicio puede activar el uso obligatorio de autenticación de doble factor a través del panel de administración de la nube, de modo a que cada usuario de una cuenta del servicio tendrá que configurarlo luego individualmente.

Tipo de control: Funcionalidad de la plataforma

Herramientas: depende de la plataforma (teléfono, Google Authenticator, etc.)

Tiempo estimado: 2 a 3 minutos por plataforma

Personal necesario: 1 persona.

Conocimiento técnico: ninguno

Costo: ninguno

Enlace: https://support.office.com/es-es/article/Configurar-la-autenticaci%C3%B3n-multifactor-para-los-usuarios-de-Office-365-8f0454b2-f51a-4d9c-bcde-2c48e41621c6

3. Configuración de información de recuperación:

Las plataformas de servicios en la nube también permiten establecer información de recuperación (correo alternativo, teléfono, pregunta de seguridad, etc.) de modo a que, si se pierde el acceso a la cuenta, por el motivo que sea, se pueda recuperar el acceso. Cada administrador de la cuenta del servicio debe asegurarse de haber completado de manera correcta esta información.

Sistemas internos:

Debido a la diversidad de sistemas que pueden existir, no es posible modelar una implementación estándar de los controles propuestos, ya que éstas serán sumamente diversas, por lo que no se ha probado la implementación de los mismos.

Servidores propios:

1. Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.):

Opción 1:

Para servidores Linux, algunos softwares de seguridad son ClamAV (antivirus/antimalware), rkhunter, chrootkit (antirootkit), todos gratuitos. Pueden ser configurados para ejecutarse automáticamente de manera periódica y enviar reportes al administrador.

Tipo de control: Herramienta de nivel de equipo

Herramientas: ClamAV, rkhunter o chrootkit

Tiempo estimado: 10 a 20 minutos por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio

Costo: ninguno

Enlace:

https://www.clamav.net/downloads

https://www.cyberciti.biz/faq/howto-check-linux-rootkist-with-detectors-software/

Opción 2:

Para Windows Server:

Tipo de control: Herramienta de nivel de equipo

Herramientas: Kaspersky Windows Server Security o Security 10 for Windows Server, Bitdefender fow Windows Server o for File Server (Windows), Symantec Endpoint Protection Small Business Edition, u otros

Tiempo estimado: 30 minutos a 1 hora por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio a avanzado

Costo: desde 30 a 300 USD por servidor

2. Firewall basado en Host y/o en red:

Opción 1:

Como firewall a nivel de host, para servidores Windows se puede utilizar el firewall de Windows y para servidores Linux se puede utilizar *iptables*, ambos sin costo. Se debe modelar las reglas de modo a permitir solo las conexiones entrantes a los puertos de servicios que deben estar expuestos y denegar las demás; en caso de que algún servicio deba estar expuesto solo desde un origen determinado (por ejemplo, solo desde la LAN o solo desde otro servidor) se debe permitir las conexiones entrantes desde ese único origen. Por lo general, se configura el firewall para permitir todas las conexiones salientes del servidor, sin embargo, teniendo en cuenta que el servidor raramente necesite iniciar conexiones (para actualizarse, para descargar un paquete, para conectarse a una base de datos, etc.), se puede limitar las conexiones a puertos y/o destinos conocidos, únicamente.

Tipo de control: Herramienta de nivel de equipo

Herramientas: Iptables (Linux) o firewall de Windows (Windows Server)

Tiempo estimado: 5 a 10 minutos para la instalación, 30 a 45 minutos para configuración granular

Personal necesario: 1 persona.

Conocimiento técnico: intermedio a avanzado

Costo: ninguno

Enlace: https://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/

Opción 2:

pfSense es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Router, entre otras funcionalidades. Es gratuito y puede ser instalado en una PC-servidor de bajas prestaciones o incluso en una máquina virtual; también están disponibles en versión *appliance* físico desde 150 USD

Tipo de control: Herramienta a nivel de red

Herramientas: pfSense (opcional, *appliance* pfSense)

Tiempo estimado: 1 a 2 horas

Personal necesario: 1 persona.

Conocimiento técnico: avanzado

Costo: ninguno (*appliance* físico desde 150 USD)

Enlaces:

https://www.pfsense.org/download/

https://www.bellera.cat/josep/pfsense/regles_cs.html

3. IDS/IPS basado en Host y/o en red:

Opción 1:

Fail2ban es una herramienta gratuita para Linux que protege principalmente contra ataques de fuerza bruta y otras actividades maliciosas contra servicios como SSH, cuentas de correo, servidor web, etc, a través del bloqueo de las IPs que originan el tráfico malicioso. La configuración por defecto suele ser suficiente para las necesidades de una PYME, sin embargo, puede ser personalizada.

Tipo de control: Herramienta a nivel de equipo

Herramientas: fail2ban

Tiempo estimado: 10 a 15 minutos por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio a avanzado

Costo: ninguno

Enlace: https://linode.com/docs/security/using-fail2ban-for-security/

Opción 2:

Snort es un IDS/IPS a nivel de red gratuito, de código abierto y uno de los más utilizados en todo tipo de organizaciones, en todo el mundo. Puede ser instalado en un equipo dedicado; sin embargo, pfSense ofrece el paquete de Snort y de Suricata (un *fork* de Snort) entre sus utilidades, debiendo ser activado simplemente. Las reglas de un IDS/IPS, especialmente a nivel de red, deben ser personalizadas o ajustadas de acuerdo a la necesidad de la empresa, de lo contrario se corre el riesgo de que se bloqueen intentos legítimos de conexión, lo que puede ocasionar problemas. La configuración inicial es adecuada para muchos escenarios, pero el ajuste de las reglas requiere mucho tiempo y conocimiento antes de ser implementado de forma definitiva. Requiere una administración casi permanente.

Tipo de control: Herramienta a nivel de red

Herramientas: pfSense, Snort o Suricata

Tiempo estimado: 20 a 30 minutos para la activación y configuración inicial (se asume que pfSense ya se encuentra implementado correctamente) – 2 a 3 meses de monitoreo, configuración y ajuste adicional

Personal necesario: 1 persona.

Conocimiento técnico: avanzado

Costo: ninguno

Enlace:

https://doc.pfsense.org/index.php/Setup_Snort_Package

4. Actualización de sistema operativo y programas:

Opción 1:

En el caso de servidores Linux existen herramientas de automatización de actualización (yum-cron o similar), tanto del sistema operativo como de los paquetes descargados de repositorios oficiales; se debe tener en cuenta que, en caso de software instalado desde orígenes distintos, debe verificarse y/o actualizarse manualmente. En distribuciones específicas para servidores y de alta estabilidad, como CentOS/RHEL o Ubuntu LTE, los problemas de compatibilidad son muy raros.

Tipo de control: Herramienta a nivel de equipo

Herramientas: yum-cron o similar

Tiempo estimado: 5 a 10 minutos por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio

Costo: ninguno

Enlace:

https://www.thegeekdiary.com/centos-rhel-configure-yum-automatic-updates-with-yum-cron-service/

https://www.techrepublic.com/article/automatically-update-your-ubuntu-system-with-cron-apt/

Opción 2:

En el caso de servidores Windows, la actualización se puede realizar de la misma manera que como se realice en los equipos Windows, ya sea a través de Windows Update combinado con actualización manual de los demás componentes o a través de una herramienta de gestión de vulnerabilidades.

5. Protección de servicios expuestos con contraseñas robustas:

En algunos servicios se permite establecer políticas de contraseña, sin embargo, en otros, dependerá del usuario. En caso de RDP (servidores Windows) las políticas de contraseña se gestionan a partir de las políticas del sistema operativo, ya que las credenciales de acceso son las mismas del equipo. En el caso de SSH (servidores Linux, principalmente) las políticas de contraseña se establecen en el archivo de configuración del servicio SSH.

Tipo de control: Funcionalidad del sistema operativo o servicio

Herramientas: ninguna

Tiempo estimado: 5 a 10 minutos por servicio

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno

6. Hardening de sistema operativo y de servicios expuestos:

Opción 1:

Se puede realizar un hardening de manera manual, eligiendo alguna guía como por ejemplo CIS Benchmarks. Algunas de las medidas de protección que se implementan en el proceso de hardening es deshabilitar los usuarios administrativos, limitar los intentos de acceso fallido, desinstalación de paquetes innecesarios, establecimiento de políticas de contraseña robusta, restricción de permisos a lo estrictamente necesario, etc. Los cambios pueden incorporarse gradualmente.

Tipo de control: Procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 2 a 8 horas por servidor

Personal necesario: 1 persona

Conocimiento técnico: avanzado

Costo: ninguno

Enlace: https://www.cisecurity.org/cis-benchmarks/

Opción 2:

Se puede realizar un hardening de manera automatizada o semi-automatizada con OpenSCAP, una herramienta basada en *baselines* ampliamente aceptados por la industria, para varios sistemas operativos y usos comunes. Consta de dos fases: primeramente, un escaneo inicial del servidor a ser protegido, en el que se identifican potenciales problemas, seguida de la fase de corrección, en la que se puede aplicar las correcciones que se desean, de manera manual, siguiendo las recomendaciones de la herramienta (incluye tutoriales específicos, paso a paso, de cómo aplicar la corrección) o se puede optar por la aplicación automatizada de las correcciones. Con el OpenSCAP Framework se puede auditar las máquinas de manera remota y centralizada.

Tipo de control: Herramienta a nivel de equipo

Herramientas: OpenSCAP framework, OpenSCAP Scanner y baselines

Tiempo estimado: 30 minutos por servidor

Personal necesario: 1 persona

Conocimiento técnico: intermedio - avanzado

Costo: ninguno

Enlace:

https://www.open-scap.org/tools/

https://www.open-scap.org/getting-started/

http://networksandservers.blogspot.com/2017/03/linux-hardening-with-openscap.html

7. Copia de seguridad continua del sistema operativo (imágenes o *screenshots* de S.O.):

Opción 1:

Rsync es una de las herramientas de sincronización más conocidas y versátiles para servidores Linux que permite realizar una copia de seguridad de manera periódica e incremental. Funciona por línea de comandos y permite realizar sincronización remota, en un modelo cliente-servidor.

Tipo de control: Herramienta a nivel de equipo

Herramientas: rsync

Tiempo estimado: 20 a 30 minutos para instalación y configuración de servidor de almacenamiento y 10 a 15 minutos por servidor (cliente)

Personal necesario: 1 persona

Conocimiento técnico: intermedio - avanzado

Costo: ninguno. Obs.: requiere un dispositivo de almacenamiento externo, ya sea físico o virtual donde copiar los archivos (servidor rsync)

Enlace: https://everythinglinux.org/rsync/

Opción 2:

Existen herramientas de sincronización similares a rsync para servidores Linux, pero con interfaz gráfica, como por ejemplo Simple Backup Suite.

Tipo de control: Herramienta a nivel de equipo

Herramientas: Simple Backup Suite (sbackup)

Tiempo estimado: 15 a 20 minutos por servidor

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno. Obs.: requiere un dispositivo de almacenamiento externo, ya sea físico o virtual donde copiar los archivos.

Enlaces:

https://help.ubuntu.com/community/BackupYourSystem/SimpleBackupSuite

www.educa.jccm.es/educa-jccm/cm/images?idMmedia=92607

Controles transversales:

1. Educación al usuario:

Opción 1:

INCIBE cuenta con una serie de recursos para concienciación y sensibilización de usuarios de una empresa, para el desarrollo de una cultura en seguridad. Entre estos recursos se encuentran infografías, videos, cuestionarios de auto-evaluación y cursos masivos a distancia (MOOC)

https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

Opción 2:

El CERT-PY, de Paraguay, cuenta con una serie de iniciativas para la concienciación y sensibilización de usuarios de empresas, entre ellas, un taller mensual abierto a todo público en la que se abarca la gran mayoría de los temas específicos vinculados a usuarios de la tecnología e Internet, de manera no técnica y con énfasis en herramientas y medidas de protección al alcance del usuario. El taller tiene una duración de 3 horas y los materiales son públicos. Este mismo taller está disponible en formato de curso virtual, abierto a todo público (previo registro), y con un enfoque teórico-práctico, que le permite al usuario

entender la problemática y le guía a través de la implementación de las medidas de protección que están a su alcance.

https://www.cert.gov.py/index.php/download_file/view/565/209
http://cursos.gov.py/categorias/area-informatica/seguridad-en-internet

2. Utilización de gestor de contraseña:

Opción 1:

Un posible gestor de contraseña gratuito es Kaspersky Password Manager.

Tipo de control: Herramienta de nivel de equipo

Herramientas: Kaspersky Password Manager

Tiempo estimado: 5 minutos

Personal necesario: 1 persona para la instalación en todos los dispositivos o cada empleado lo instala individualmente.

Conocimiento técnico: básico

Costo: ninguno

Enlaces:

https://www.kaspersky.com/password-manager

https://support.kaspersky.com/sp/5271

Opción 2:

Un posible gestor de contraseña gratuito y online es LastPass, una extensión para la gran mayoría de los navegadores. También tiene una versión offline, para escritorio.

Tipo de control: Herramienta de nivel de equipo

Herramientas: LastPass

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona para la instalación en todos los dispositivos o cada empleado lo instala individualmente.

Conocimiento técnico: básico

Costo: ninguno

Enlaces:

https://lastpass.com/misc_download2.php

https://helpdesk.lastpass.com/es/