GUÍA DE CIBERSEGURIDA

25 medidas para su PYME

Contenido

Hola,

Estamos encantados de ofrecerle esta guía de buenas prácticas en ciberseguridad para su VSE o PYME.

En esta guía, hemos reunido las medidas más interesantes para poner en marcha en tu negocio, incluidas las de la ANSSI. Nuestro objetivo es que pueda empezar a implantar su ciberseguridad con esta sencilla guía.

Justo al comienzo de su lectura, hemos incluido una **«Lista de comprobación My CyberNum»** para guiarle de forma rápida y sencilla en la implantación de la ciberseguridad en su empresa. Le recomendamos que la imprima.

Disfrute de la lectura.

El equipo BETANUM

Ciberseguridad

Mi lista de control CyberNum

Formo a mis empleados en ciberseguridad

- Organizar la formación **inmediatamente después de contratar a una persona**
- Organizar al menos **1 sesión de formación al año para mis empleado**s, con seguimiento a lo largo del año.
- Ofrezca periódicamente campañas de **phishing y cursos de aprendizaje electrónico**

Pongo en marcha una estrategia

- **Gestionar rigurosamente el acceso a la creación y supresión de las cuentas de mis usuarios.**
- **Definir reglas para mis contraseñas y aplicarlas**
- **Limitar el acceso a mis datos sensibles**

Controlo mi acceso

- Configurar la identificación de **dos factores**
- **Guardar las contraseñas en una caja fuerte electrónica**
- Establecer el **acceso nominativo**

Protejo mis sistemas y redes

- **Actualizar periódicamente** el software y los sistemas operativos
- **Utilizar un cortafuegos** para proteger la red interna
- Instalar y actualizar mi **software antivirus y antimalware**

Betanum

Mi lista de control CyberNum

Protejo mis puestos de trabajo móviles

- Utilización de un **túnel VPN IPsec**
- Creación de un **archivo de dispositivos móviles**

Protejo mis datos

- Crear un **plan regular de copias de seguridad para mis datos críticos**
- Almacenar mis **copias de seguridad** fuera de las instalaciones y/o en la nube.

Dispongo de un plan de incidentes

- I**dentificar y notificar rápidamente** los incidentes de seguridad
- **Definir los pasos para responder** a un incidente

Regularmente audito y optimizo

- Saber cómo llevar a cabo **evaluaciones de riesgos periódicas**
- Establecer **auditorías de seguridad para comprobar la conformidad** de mi sistema informático

Betanum

Etapa 1
Forme a sus empleados en ciberseguridad

1 Eduque a sus nuevos reclutas

Según Statista, el 74% de los ciberataques tienen su origen en el phising. Por tanto, todos los empleados deben estar informados desde su incorporación a la empresa para aumentar las posibilidades de éxito. Por tanto, es esencial formar a los nuevos empleados e informarles de los riesgos del phishing y de las normas de seguridad informática que deben respetar desde su llegada. **Lo ideal es organizar sesiones de formación y concienciación lo antes posible durante el proceso de incorporación.**

Además, las sesiones deben impartirse con regularidad, adaptarse a las distintas personas y ofrecerse de distintas formas. **Pueden adoptar la forma de formación sobre phishing por correo electrónico, formación presencial o e-learning.** Además, puedes establecer una carta de seguridad y hacer que la firmen. Los distintos temas tratados pueden ser :

- Objetivos de seguridad de su empresa
- Phishing
- Normas que deben cumplirse (por ejemplo, NIS 2)
- Información sensible
- Normas internas de ciberseguridad que deben cumplirse (por ejemplo, no utilizar las contraseñas del trabajo en la vida diaria)
- Herramientas disponibles para la ciberseguridad de su empresa

2 Forme regularmente a sus empleados

Hoy en día, muchos empleados pueden tener acceso a datos privilegiados que no siempre se adaptan a sus necesidades. Esto puede suponer un riesgo para la ciberseguridad.

Es esencial ofrecer **formación periódica en seguridad informática a los equipos operativos y de gestión, así como a los subcontratistas.**

Le recomendamos que realice campañas periódicas de phishing y que forme a su personal **al menos una vez al año.**

Puede hacer que la ciberseguridad **forme parte de su objetivo profesional anual.**

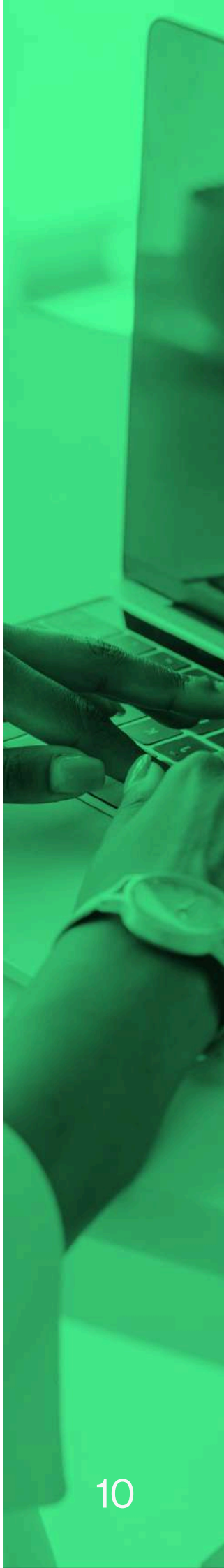
Estos son los posibles temas:
- Control de acceso
- Cuestiones de empresa
- Los riesgos
- Mantenimiento de la seguridad
- Normas internas
- Nueva legislación
- Configuración del sistema y de la red

Etapa 2
Aplicar una estrategia de seguridad

3 Establezca sus reglas de contraseña

Puede establecer distintas reglas de seguridad de contraseñas para elegir y dimensionar las contraseñas en su empresa.

- **Conciencie a sus usuarios de los riesgos de utilizar** una contraseña demasiado simple o de reutilizar una contraseña para otra plataforma.
- **Cambie regularmente** sus contraseñas.
- **Bloquear cuentas tras varios** intentos de contraseña.
- **Implantar una herramienta de auditoría** que reconozca la solidez de las contraseñas.



4 Limitar el acceso a datos sensibles

Su empresa tiene información sensible. Puede ser sobre sus clientes, su negocio o sus innovaciones. Necesita identificar esta información para proteger su empresa.

Le recomendamos que elabore una lista y, a continuación, identifique los elementos del sistema y dónde se encuentran (archivos compartidos, bases de datos, etc.). Estos elementos constituyen riesgos. Por eso es importante poner medidas. Puede tratarse de copias de seguridad, acceso, etc.

Este ex-servicio le dará un mapa de zonas con IPs, equipos, servidores y conexiones.

5 Organizar la creación y eliminación de cuentas

Su plantilla cambia constantemente. Esto puede implicar salidas, llegadas o movilidad interna. **Por eso es importante actualizar periódicamente los derechos y accesos de los usuarios.**

Por lo tanto, es necesario definir las instrucciones de salida y llegada y vincularlas a su función.

Estas instrucciones deben tener en cuenta lo siguiente :

- Derechos de administración
- Buzones de correo electrónico
- Teléfonos móviles, tabletas, memorias USB, etc.
- Contraseñas
- Cuentas informáticas
- Acceso a los locales
- Acceso a los documentos...

6 Reducir el acceso a cuentas privilegiadas

Las cuentas de usuario con privilegios específicos son objetivos prioritarios para los ciberatacantes que buscan obtener un mayor acceso al sistema de información. Por lo tanto, hay que estudiarlas con mucha atención. Es esencial crear inventarios de estas cuentas, mantenerlos actualizados, incluir la siguiente información y crear categorías:

- E**n primer lugar, los usuarios que tienen derechos suficiente**s para acceder a los directorios de trabajo de los gestores o de todos los usuarios.
- Usuarios con **cuentas de administrador o derechos superiores** a los de un usuario estándar.
- **Usuarios cuyas estaciones de trabajo no son gestionadas por el departamento de TI** y no están sujetas a las medidas de seguridad de la política de seguridad general de su empresa.

Es aconsejable organizar reuniones **periódicas de estas cuentas** para comprobar que el acceso a los elementos sensibles se gestiona correctamente.

Por último, es importante establecer una **clasificación simplificada para reconocer las distintas cuentas**. Esto simplificará su análisis.

Etapa 3
Controle su acceso

7 Configurar la autenticación de dos factores

Se recomienda configurar la autenticación de **dos factores (2FA)** para que su empresa sea más segura.

Hay varios factores entre los que elegir:

- **Algo que sabe:** contraseña, contraseña de un solo uso, PIN.
- **Algo que tiene:** token, llave/tarjeta inteligente, tarjeta inteligente.
- **Algo que es:** huella dactilar.

Las tarjetas inteligentes y las contraseñas de un solo uso con tokens logran buenos resultados de seguridad.

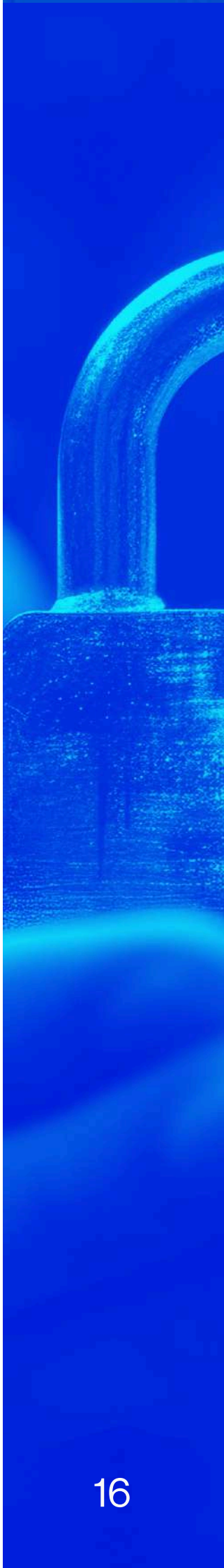
8

Guarde sus contraseñas en una caja fuerte digital

Hoy en día, tenemos que utilizar varias contraseñas para acceder a nuestras plataformas. Este uso complejo nos incita a guardarlas bien en una hoja de notas, en notas post-it o en un archivo digital.

Sin embargo, hay que estar en guardia contra los ciberatacantes.

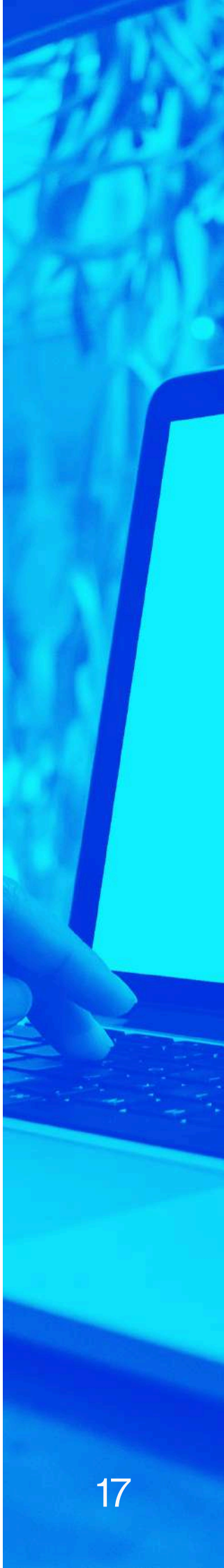
Es aconsejable guardar las contraseñas en una **caja fuerte digital** o con mecanismos de encriptación. De esta forma, sólo tendrás que recordar una contraseña y tu negocio estará más seguro.



9 Crear cuentas de acceso personales

Las cuentas que dan acceso al sistema de información deben ser nominativas, para ofrecer una respuesta eficaz y rápida en caso de problema :

- En primer lugar, le recomendamos que limite el número de cuentas **genéricas de «administrador».**
- **Las cuentas genéricas deben formalizarse y gestionarse estrictamente.**
- La cuenta de administración sólo se utilizará para **acciones de administración.**

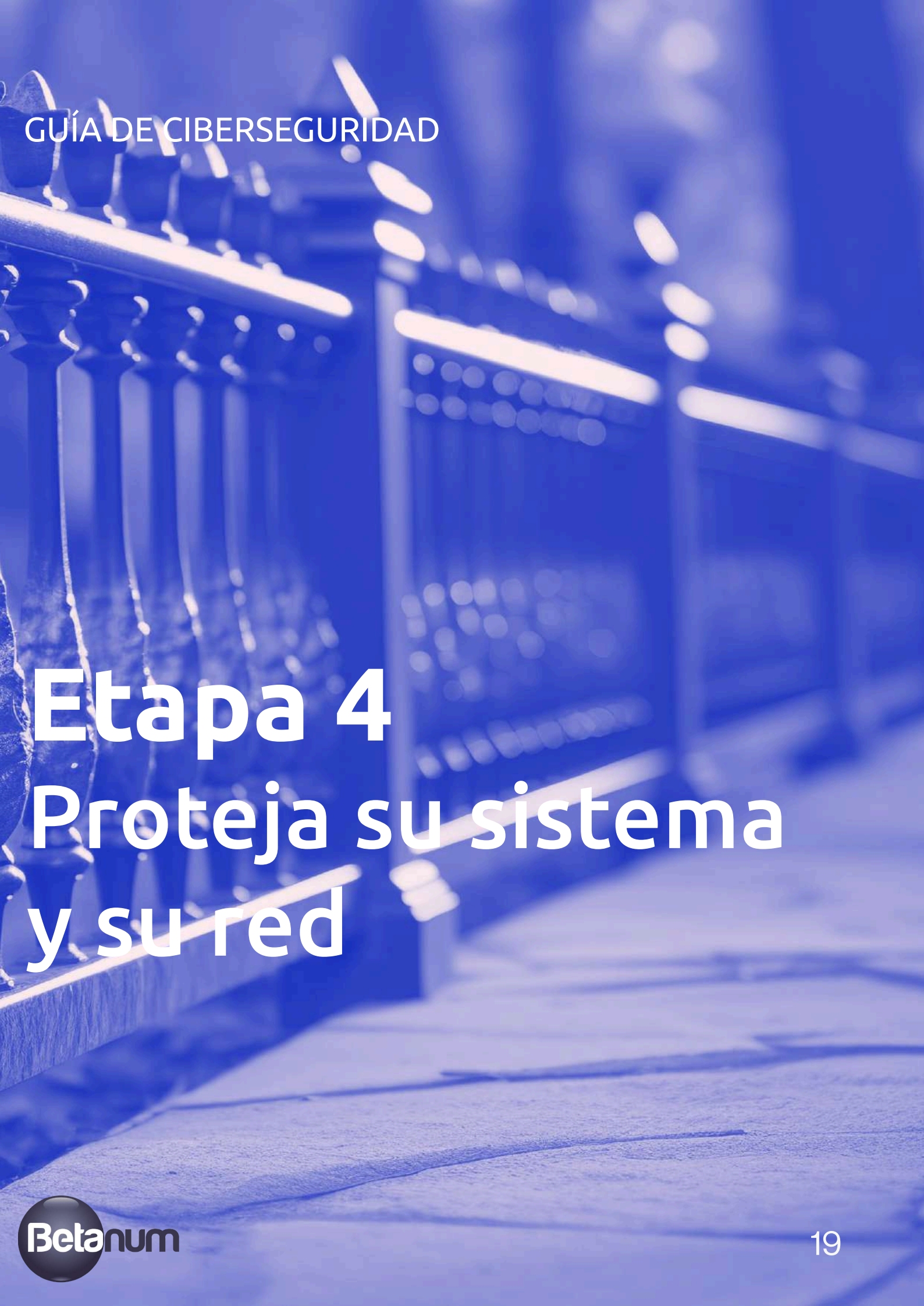


10 Modificar el acceso a los servicios por defecto

Sus configuraciones por defecto son conocidas por los ciberatacantes.

A menudo son demasiado simples (contraseñas comunes entre cada plataforma, demasiado débiles, etc.) y accesibles a los atacantes.

- Le recomendamos que :
- **Modificar las configuraciones** en cuanto disponga de una nueva herramienta
- Implantar los **nuevos procedimientos de seguridad** de su empresa
- Renovar los **accesos con regularidad.**



Etapa 4
Proteja su sistema y su red

11 Actualice sus programas y sistemas con los últimos parches

Puede reducir el riesgo de intrusión actualizando periódicamente sus programas y sistemas con los últimos parches de seguridad. Así sus sistemas serán menos vulnerables.

Para ello, puede:

- Automatizar todas las actualizaciones
- Supervisar los avisos de seguridad
- Auditar los sistemas con regularidad
- Formar a los usuarios

12 Utilice un cortafuegos de Internet seguro

Sus empleados pueden descargar archivos peligrosos o visitar sitios con código malicioso, por ejemplo. Como resultado, sus datos podrían filtrarse. Para proteger su acceso a Internet, le recomendamos que sus terminales de usuario no tengan acceso directo a Internet:

- Configurar un acceso seguro a Internet con un **cortafuegos cerca de la conexión** a Internet para depurar las conexiones y un servidor proxy con procesos de seguridad para analizar las autenticaciones.
- **Realizar trabajos adicionales en el servidor, como auditorías antivirus.**
- Mantener la seguridad de los equipos de la pasarela con los procesos que se pongan en marcha.
- **Desactivar DNS** vinculados directamente a nombres de dominio públicos.
- **Separe las conexiones Wi-Fi de los puestos nómadas de las de la entidad** (SSID y VLAN deben estar separados) y permita que los puestos nómadas accedan a Internet a través de la pasarela.

13 Compruebe la seguridad de sus redes Wi-Fi

Utilizar Wi-Fi en el lugar de trabajo es ya de rigor, pero existen amenazas para la seguridad informática. Por ejemplo, la disponibilidad aleatoria de Wi-Fi podría dar lugar a un ciberataque..

Para optimizarlo, aquí tienes algunas cosas que debes poner en práctica:

- **Divida su arquitectura de red para limitar el acceso a un perímetro determinado.**
- Ordene los elementos importantes que debe conservar para sus puestos de trabajo conectados a Wi-Fi.
- Establecer un cifrado muy fuerte y una autenticación centralizada.
- Proteja su Wi-Fi con una **contraseña completa** que se renueve periódicamente y que no se comparta internamente.
- Distribuya los puntos de acceso de forma segura a través de una **interfaz dedicada a un administrador de su organización**
- **Separe las conexiones Wi-Fi de los terminales personales de su empresa (SSID, VLAN)**
- **Crear Wi-Fi para invitados**

14 Proteja su correo electrónico

Enviar un correo electrónico representa un riesgo importante para la ciberseguridad, ya sea al abrir archivos adjuntos o al hacer clic en un enlace a un sitio hostil. Aquí tienes algunas cosas que puedes hacer:

- Por tanto, es esencial **sensibilizar a sus empleados y a los recién llegados**. Deben preguntarse: ¿conozco a esta persona? ¿Espero algo de esta persona?
- No redirija los **correos electrónicos de trabajo a correos personales**, para evitar la fuga de datos.
- **Aloje su sistema de correo electrónico, configure un análisis antivirus** de los buzones y active el cifrado TLS de los servidores de correo electrónico, los servidores de buzones y las estaciones de trabajo de los usuarios.

15 Instalar soluciones antivirus en todas las estaciones de trabajo

Las soluciones antivirus son esenciales para protegerle de los ciberdelincuentes.

- Para empezar, **elija un software antivirus**, que podría ser: Norton, Kaspersky, McAfee.
- Luego **instale el software** en cada ordenador.
- Y **configure los parámetros** de seguridad.
- **Mantenga el sistema actualizado.**
- **Asegúrese de que su personal** es consciente de los riesgos.

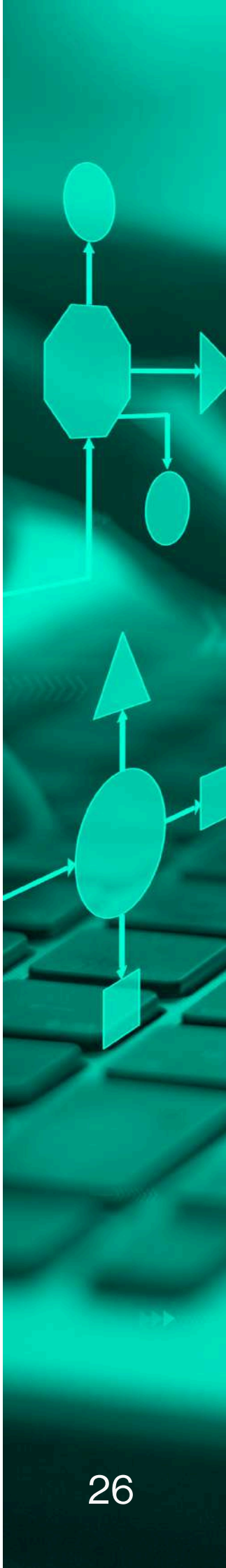
Etapa 5
Proteja sus puestos de trabajo móviles

16 Configurar un túnel VPN IPsec

Cuando uno de sus empleados se ausenta con su equipo informático, a menudo necesita acceder a la red de su empresa. Por eso es importante poder asegurar este acceso a través de Internet.

He aquí algunas recomendaciones:

- **Establezca un túnel VPN IPsec entre el puesto de trabajo externo del empleado** y una pasarela VPN IPsec propuesta por su empresa y creada automáticamente.
- Si no desea que el sistema se configure automáticamente, puede configurarlo a petición, pero debe tener cuidado, o puede pedir a su empleado que utilice una **conexión compartida en su teléfono.**
- **Autenticación robusta,** si es posible utilizando una tarjeta inteligente, un token USB o una contraseña muy segura, o incluso una contraseña de un solo uso.



17 Crear un archivo de dispositivos móviles

Sus empleados pueden perder sus equipos informáticos si están a menudo fuera de casa. Sus datos sensibles podrían estar en peligro.

Para ello, puede :

- **Almacenar sólo equipos móviles** que hayan cifrado sus datos (el usuario establecerá contraseñas seguras para las distintas herramientas utilizadas).
- **Comience por cifrar todo el disco antes de cifrar los archivos**

Etapa 6
Haga una copia de seguridad de sus datos

18 Aplicar un plan de acción de datos críticos

Poner en marcha un plan de copias de seguridad de sus datos críticos es esencial para que su PYME pueda seguir funcionando en caso de incidente.

Aquí tienes algunos pasos para configurarlo:

- **Analice y enumere sus datos críticos.**
- Elija el método de **copia de seguridad** (completa, parcial, en función de su última copia de seguridad): le aconsejamos que haga una copia de seguridad de todos sus datos.
- **Elige dónde quieres almacenar** tus datos: discos duros, nube, etc.
- **Configure su copia de seguridad** con el software de su elección (Acronis, Veem...).
- **Almacenar fuera del sitio con una copia en la nube, por ejemplo en otra ubicación geográfica.**
- **Probar la restauración.**
- **Planifique su copia de seguridad** (diario, mensual...).
- **Realizar auditorías de las copias de seguridad.**

19 Mantenga las copias de seguridad fuera del sitio y/o en la nube

Para garantizar a su empresa un alto nivel de seguridad de sus datos, es aconsejable establecer copias de seguridad fuera del sitio principal y también en la nube. Si puedes hacer ambas cosas, aún mejor.

- **Para las copias de seguridad externas,** puedes utilizar discos duros, centros de datos o almacenes seguros. Si tienes otra oficina, puedes enviar tus datos a esa oficina.
- **Puedes hacer copias de seguridad de tus datos en la nube** utilizando Amazon (AWS), Microsoft Azure o Google Cloud.

También puedes utilizar soluciones híbridas, **mezclando copias de seguridad externas y en la nube**.

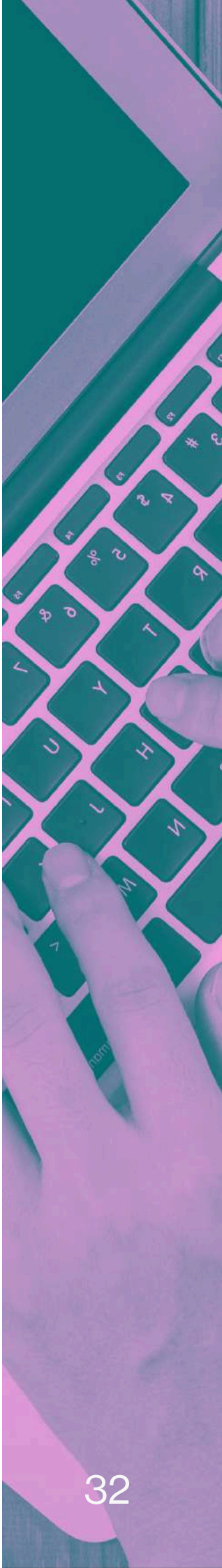
Etapa 7
Poner en marcha un plan de gestión de incidentes

20 Identificar y notificar incidentes

Saber cómo identificar y notificar un incidente es una parte importante para garantizar la seguridad de su PYME.

He aquí algunos pasos importantes:

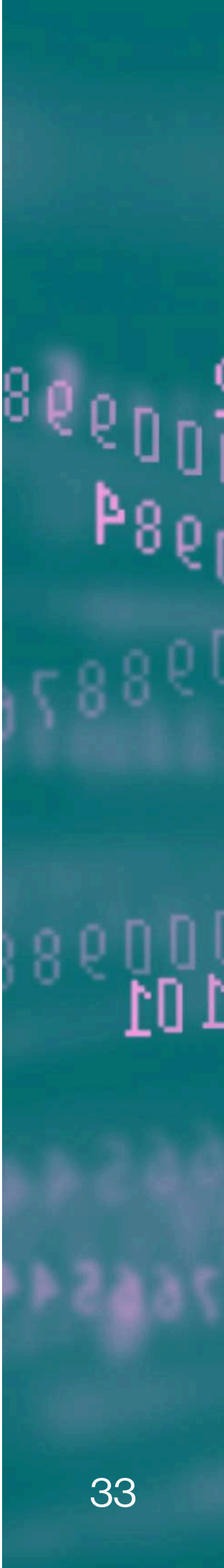
- **Identificar y elegir soluciones de detección, supervisión y antivirus.**
- Establezca procedimientos de **supervisión continua** con alertas automáticas y cuadros de mando.
- Instalar un sistema de gestión de eventos e información de seguridad con un SIEM.
- **Forme y sensibilice a su personal.**
- **Establecer un plan de respuesta a incidentes** y comunicarlo a un equipo especializado.
- **Elaborar un informe posterior al incidente,** analizando los siguientes elementos.
- Establecer **simulaciones.**

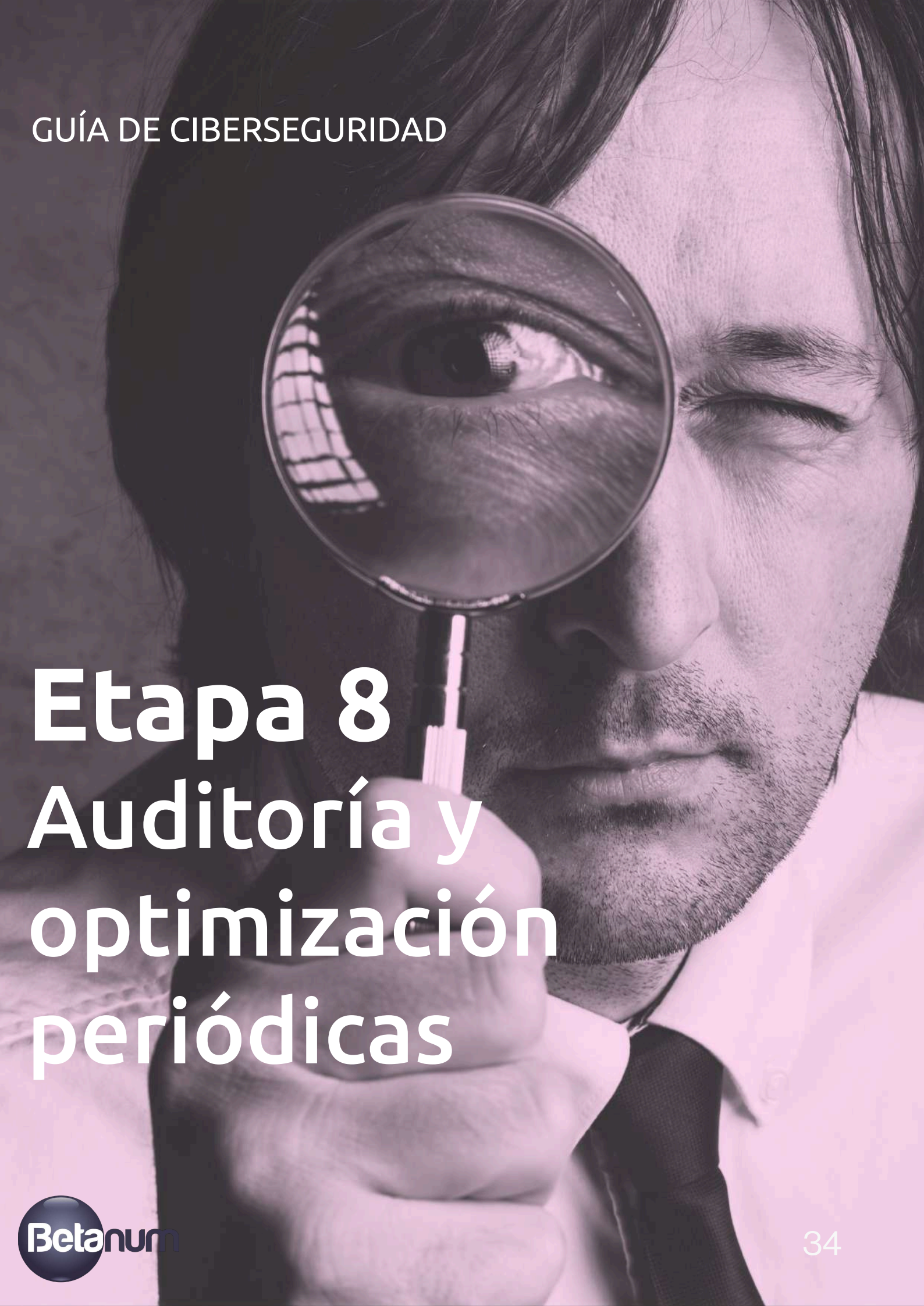


21 Defina las etapas y recupere sus datos

He aquí algunos pasos para definir su plan de acción y recuperar sus datos:

- **Establezca sus objetivos en caso de incidente.**
- Identifique los posibles tipos de incidentes (físicos, ciberataques, fugas de datos...).
- **Cree su equipo** de respuesta con responsables y defina las funciones.
- Identifique sus activos críticos.
- I**nstale herramientas de detección** (antivirus, supervisión de la red...).
- **Cree procedimientos** de respuesta inmediata.
- **Analice y evalúe.**
- **Comunique los protocolos.**
- **Restaure los sistemas.**
- **Recuperar los datos** mediante copias de seguridad.





Etapa 8
Auditoría y optimización periódicas

22 Audite periódicamente su seguridad

Le recomendamos que realice auditorías periódicas de su empresa para comprobar que su seguridad está a la altura.

Estos son los pasos:

- Planifique una **auditoría interna.**
- **Recopile información**, en particular, examine las nuevas normas vigentes en su sector y compruebe si su sistema cumple, por ejemplo, la ley RGPD o próximamente la directiva NIS.
- **Detecte los puntos débiles** y las lagunas de su red con análisis de vulnerabilidades y Pentest.
- Elabore un i**nforme de auditoría.**
- **Implemente un plan** de acción.
- **Siga** el plan de acción.
- **Refuerce la auditoría de seguridad al menos 2 veces al año.**

23 Definir una estrategia de mantenimiento

Es probable que observe nuevas vulnerabilidades en sus sistemas informáticos. Esto podría suponer una oportunidad para que un ciberatacante irrumpa en ellos.

Para protegerse, es esencial contar con una estrategia de actualización periódica con diferentes procedimientos.

Estos son los elementos que deben especificarse:

- La forma en que se ha realizado **la evaluación del sistema informático.**
- **La calidad de las correcciones** y su desarrollo en los sistemas.
- El origen de la información relativa a **las actualizaciones.**
- El equipo utilizado para aplicar las **correcciones en el hardware.**

24 Anticiparse a la obsolescencia

Un sistema de información obsoleto aumenta el riesgo potencial de intrusión por un ciberataque, ya que las optimizaciones han dejado de existir.

He aquí algunas formas de protegerse:

- Actualice un **inventario de todos los sistemas y aplicaciones de su empresa.**
- Seleccione únicamente herramientas que **garanticen un plazo que se corresponda con su uso.**
- Tenga una **única versión de cada programa informático.**
- Congele las **suscripciones a programas informáticos**.
- Recuerde las **fechas de finalización** de los programas informáticos que debe cambiar.
- Tenga **contratos que garanticen** la gestión de la obsolescencia de sus materiales.

25 Nombramiento de un responsable interno de seguridad

Es esencial que haya alguien en su empresa que sea responsable de sus sistemas de información.

- Esta persona será **identificada por todos sus empleados.**
- Definirá los **distintos procedimientos.**
- **Revisará la aplicación de las normas.**
- **Sensibilizará a los empleados** y podrá establecer un plan de formación.

Deberán estar formados en seguridad informática y estar en condiciones de señalar los problemas encontrados por los empleados y responder a las necesidades de sensibilización. Por último, pero no por ello menos importante, estarán motivados por el hecho de que sus resultados en materia de ciberseguridad se evaluarán anualmente.

Gracias por leer esta guía. Esperamos que le haya resultado útil.

Si desea llevar su ciberseguridad aún más lejos, estaremos encantados de ayudarle.

Puede ponerse en contacto con nosotros en el +34 625 224 213 o por correo electrónico contact@betanum.com

Hasta pronto.

El equipo BETANUM