Uso de wifi y redes externas

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. USO DE WIFI Y REDES EXTERNAS

1.1. Antecedentes

Es habitual tener que acceder a los datos de la empresa cuando estamos fuera del lugar de trabajo (viajes, reuniones, teletrabajo, etc.). En ocasiones no podemos hacer uso de las redes o conexiones 4G/5G, lo que nos obliga a conectarnos a redes domésticas o a redes públicas (hoteles, cafeterías, aeropuertos, etc.) que en la mayoría de los casos podrían no ser seguras.

Es prudente asumir que, por defecto, las redes inalámbricas que utilizan los trabajadores fuera del entorno empresarial, no disponen de las medidas de seguridad necesarias para la protección de los datos y las comunicaciones corporativas. A menudo, la información confidencial de nuestra empresa se transmite a través de **redes inalámbricas** cuya seguridad no está bajo nuestro control, por lo que debemos asegurarnos de que los datos viajan convenientemente protegidos [13] antes de hacer uso de estas redes.

La empresa debe establecer las condiciones y circunstancias en las que se permite el acceso remoto a los servicios corporativos. Es decir, determinar quién puede acceder a qué, cómo y cuándo. Esta tarea implica disponer de los medios necesarios para llevarla a cabo y ofrecer la correspondiente formación a los trabajadores para que conozcan cómo conectarse de forma segura y cómo mantener sus equipos seguros cuando viajan o se conectan desde el exterior.

Una de las herramientas de seguridad que podemos implantar para realizar accesos remotos corporativos desde el exterior de la empresa, es la utilización de una **Red Privada Virtual o VPN** [1]. Utilizaremos una VPN cuando necesitemos acceder a información confidencial de manera remota, y la red que estemos utilizando no ofrezca las suficientes garantías de seguridad. Estas son las ventajas de utilizar una VPN:

- toda la información se transmite de manera segura gracias al cifrado de datos y de conexión;
- confidencialidad e integridad de la información: al ir cifrada, la información no puede ser leída, modificada o alterada durante la transmisión;
- la información solo se trasmite entre dispositivos autorizados y configurados para este fin;
- restricción de acceso: a través de usuario y contraseña necesitando una previa autorización;
- fácil ampliación del número de usuarios.

Las conexiones establecidas utilizando VPN protegen la información que se intercambia, ya que establecen un canal cifrado de comunicación entre nuestro dispositivo y nuestro lugar de trabajo por donde «viajan» nuestros datos de manera segura.

1.2. Objetivos

Garantizar la seguridad de los datos y comunicaciones corporativos cuando el acceso a los mismos tiene lugar desde fuera de las instalaciones de la empresa mediante la utilización de redes externas no corporativas.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al **uso de wifi y redes externas**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO/TEC	**Política de conexión** Elaboras una normativa corporativa para regular las conexiones externas.	☐
A	TEC	**Configuración de la VPN** Configuras una conexión VPN para acceder desde el exterior. Creas cuentas de usuario con permisos de acceso. Detallas el software permitido para realizar estas conexiones. Estableces un tiempo de desconexión automática de la VPN tras un periodo de inactividad.	☐
B	PER	**Uso de la VPN** Conoces cómo conectarte vía VPN (si la empresa lo permite) y en qué situaciones debes hacerlo.	☐
B	PER	**Acceso a redes wifi ajenas** Al conectar a una nueva red inalámbrica, compruebas que utiliza el protocolo WPA2. Compruebas que los sitios a los que accedes tienen certificado y utilizan protocolos seguros (https://) si vas a realizar actividades críticas.	☐
A	PER	**Configuración de la wifi doméstica** Antes de utilizarlas, configuras el protocolo WPA2, y cambias el nombre del SSID y las credenciales por defecto.	☐

NIVEL	ALCANCE	CONTROL	
B	PER	**Redes inalámbricas de los dispositivos móviles** Abres las conexiones wifi y *bluetooth* de tus dispositivos móviles solo cuando se van a utilizar y para conectarte a dispositivos confiables.	☐
B	PER	**Uso de dispositivos móviles** Revisa las políticas de uso de dispositivos móviles y uso de dispositivos personales en el ámbito corporativo.	☐
B	PER	**Uso de ordenadores no corporativos** Evita el uso de ordenadores no corporativos. Revisa la seguridad de tus dispositivos domésticos y toma precauciones cuando utilices dispositivos de uso compartido.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Política de conexión** [2]**.** La dirección debe determinar si la política de seguridad permite la conexión desde redes externas a los recursos de la empresa y establecer las condiciones este tipo de accesos.
- **Configuración de la VPN.** Para los accesos permitidos desde el exterior el equipo técnico debe disponer y configurar un servicio VPN:
  - crear cuentas de usuario con permisos de acceso personalizados;
  - determinar el software permitido para realizar conexiones VPN;
  - establecer un tiempo para la desconexión automática de la VPN tras un periodo de inactividad;
- **Uso de la VPN.** Los empleados que tengan autorizado el acceso vía VPN conocerán cómo hacerlo y cuándo está permitido:
  - cuando utilicemos redes públicas o no confiables;
  - para acceder a los recursos corporativos como impresoras, documentos, servidores de base de datos, aplicaciones específicas, etc.;
  - cuando necesitemos hacer operaciones confidenciales: acceso a bases de datos, banca online o facturación, que impliquen la transmisión de usuarios, contraseñas, o cualquier otra información confidencial;
  - cuando queramos interconectar redes separadas de forma segura: distintos edificios u oficinas separadas geográficamente, equipos utilizados en teletrabajo con la oficina, etc.;
  - cuando hagamos uso del teletrabajo.
- **Acceso a redes wifi ajenas.** Al conectarte a una red inalámbrica desconocida, compruebas que utiliza el protocolo WPA2 y revisas el uso vas a hacer de esa red [7]:
  - Sólo utiliza **redes wifi púbicas no seguras** para realizar actividades de bajo riesgo como navegar o leer noticias, pero asegúrate que el canal está cifrado (sitio web con https:// y certificado) si has de iniciar sesión (hacer *login*) o suscribirte.
  - Sólo utiliza **redes wifi públicas seguras** (al menos con WPA2) si no tienes otro medio más seguro (redes móviles 4G/5G o una VPN) a tu alcance para realizar actividades de alto riesgo (uso de email, trabajar con documentos online, redes sociales, banca online o compras online) comprobando además que accedes a sitos web legítimos, cifrados (https://) y con certificado.
- **Configuración de la wifi doméstica** [3]**.** En el caso de usar una wifi doméstica, tendremos que configurarla para:
  - activar el protocolo WPA2;
  - cambiar el nombre por defecto del SSID;
  - cambiar las credenciales por defecto;
- **Redes inalámbricas de los dispositivos móviles** [4]**.** Activar la conexión wifi, *bluetooth* o antena GPS únicamente en los momentos que se vayan a utilizar y con las convenientes medidas de seguridad.
- **Uso de dispositivos móviles.** Si utilizas dispositivos móviles para trabajar fuera de la empresa, se han de tomar las medidas de seguridad indicadas en las Políticas

de uso de dispositivos móviles corporativos [14] y en la de uso de dispositivos móviles no corporativos [8].

- **Uso de ordenadores no corporativos.** Si utilizas ordenadores de uso público evita realizar actividades de alto riesgo (uso de email corporativo, trabajar con documentos online, redes sociales, banca online o compras online). Desconfía de la seguridad del equipo y sus conexiones. En cualquier caso si te vieras en la necesidad de utilizarlos para hacer *login* en algún servicio corporativo siempre que esté permitido y no puedas hacer uso de una VPN:

    - revisa el entorno para evitar la mirada de observadores o de cámaras
    - utiliza el modo de navegación privada del navegador;
    - teclea la URL o dirección web, en lugar de utilizar el buscador;
    - verifica que la página a la que accedes es auténtica, que utiliza protocolo https:// y que tiene certificado y está vigente;
    - evita que el navegador guarde las contraseñas;
    - al finalizar la sesión borra el historial de navegación y las cookies en el navegador;
    - no conectes pendrives ni otros dispositivos externos;
    - revisa que no dejas ningún archivo personal en el equipo.

  Si utilizas ordenadores domésticos:

    - actualiza el software de sistemas operativos y aplicaciones;
    - utiliza un usuario no compartido;
    - instala y activa un antivirus y el cortafuegos del sistema operativo;
    - no instales aplicaciones sin licencia o cuyo origen desconozcas.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog -¿Por qué deberías utilizar una red privada virtual y cómo hacerlo? https://www.incibe.es/protege-tu-empresa/blog/deberias-utilizar-red-privada-virtual-y-hacerlo

[2]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protección en movilidad y conexiones inalámbricas https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-movilidad-conexiones-inalambricas

[3]. Incibe – Protege tu empresa – Blog – 7 atributos que debe tener tu wifi y 9 consejos para configurarla https://www.incibe.es/protege-tu-empresa/blog/7-atributos-debe-tener-tu-wifi-y-9-consejos-configurarla

[4]. Incibe – Protege tu empresa – ¿Qué te interesa? – Incorporación segura de dispositivos móviles a la empresa https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-movilidad-conexiones-inalambricas

[5]. Incibe – Protege tu empresa – Blog – ¿Vacaciones de verano para ti? https://www.incibe.es/protege-tu-empresa/blog/vacaciones-verano-TI

[6]. Incibe – Protege tu empresa – Blog – 7 cuestiones para usar el móvil de forma segura en la pyme (1/2) https://www.incibe.es/protege-tu-empresa/blog/7-cuestiones-usar-movil-forma-segura-1

[7]. Incibe – Protege tu empresa – Blog – 7 cuestiones para usar el móvil de forma segura en la pyme (2/2) https://www.incibe.es/protege-tu-empresa/blog/7-cuestiones-usar-movil-forma-segura-2

[8]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de dispositivos móviles no corporativos https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[9]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Control de acceso https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[10]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Protección del puesto de trabajo https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[11]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en los equipos de trabajo https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[12]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en la nube https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[13]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de técnicas criptográficas https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[14]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme –Uso de dispositivos móviles corporativos https://www.incibe.es/protege-tu-empresa/herramientas/politicas

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD