Teletrabajo seguro

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. TELETRABAJO SEGURO

1.1. Antecedentes

El teletrabajo permite llevar a cabo la actividad laboral desde una ubicación distinta a la sede de la empresa. Habitualmente se realiza desde el domicilio del empleado o en otras ubicaciones cuando el empleado está fuera de su puesto de trabajo (en un medio de transporte mientras viaja, en un hotel, etc.). Las organizaciones están adoptando este método de trabajo porque les permite adaptarse a posibles situaciones excepcionales, como el confinamiento durante la pandemia, ofrecer medios para una mejor conciliación laboral o contar con talento afincado en lugares remotos.

La seguridad durante el teletrabajo está vinculada a la tecnología utilizada para el acceso remoto y para la actividad diaria. Por tanto, dependerá de los riesgos asociados a los mecanismos de acceso remoto a la red y a los servidores de la empresa, y de los relativos al uso de ordenadores de sobremesa, portátiles, teléfonos inteligentes o tabletas, medios de almacenamiento extraíbles (memorias USB, discos duros, etc.), herramientas colaborativas y aplicaciones en la nube. En ocasiones esta tecnología es compartida para usos domésticos lo que conlleva riesgos específicos.

Permitir el teletrabajo sin contar con medidas de seguridad puede ser un riesgo para la organización, ya que los empleados podrían hacer uso de aplicaciones y dispositivos no permitidos, facilitando el acceso de los ciberdelincuentes a la red de la empresa y a la información que se gestiona, poniendo en riesgo la continuidad de negocio y por ende la imagen de la empresa.

Para disponer de un entorno de teletrabajo seguro, necesitamos establecer una política de seguridad en la que se contemplen las directrices a seguir respecto al uso de los distintos sistemas y métodos de acceso, contemplando todos los posibles escenarios. Esta política debe definir las medidas necesarias para proteger los dispositivos de teletrabajo, garantizar conexiones remotas seguras, el uso seguro de la nube y de las herramientas colaborativas y la seguridad en movilidad, siempre teniendo en cuenta las necesidades particulares de cada organización.

1.2. Objetivos

Garantizar la seguridad de toda la información y los recursos gestionados cuando se teletrabaja.

Concienciar a los empleados de la importancia de cumplir las medidas de seguridad tanto dentro como fuera de la oficina.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **teletrabajo seguro**.

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	**Normativa de protección del puesto de trabajo remoto.** Informas al personal sobre la normativa de protección del puesto de trabajo fuera de la oficina llevando a cabo auditorías periódicas para asegurar su cumplimiento.	☐
B	PRO/TEC	**Relación de usuarios que disponen de la opción de trabajar en remoto.** Llevas un control de las personas que, por su perfil dentro de la empresa o las características de su trabajo, tienen la opción de teletrabajar.	☐
B	PRO/PER	**Procedimientos para la solicitud y autorización del teletrabajo.** Redactas un documento donde se contemplen todas las cuestiones relativas al teletrabajo (duración del mismo, dispositivos facilitados, etc.), que será firmado por cada teletrabajador.	☐
A	TEC	**Periodo de implantación y pruebas.** Valoras diferentes escenarios y configuraciones antes de habilitar el teletrabajo, contemplando todos los riesgos de seguridad.	☐
A	TEC	**Realizar pruebas de carga en escenarios simulados.** Si existe un volumen considerable de empleados que van a teletrabajar al mismo tiempo, valoras la carga que esto ocasiona en los sistemas internos de la empresa.	☐

NIVEL	ALCANCE	CONTROL	
A	TEC	**Aplicaciones y recursos a los que tiene acceso cada usuario.** Das acceso a cada empleado solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo de su perfil dentro de la organización. Detallas las aplicaciones permitidas así como sus condiciones de uso. Valoras la inclusión del nuevo *software* solicitado por los empleados.	☐
A	TEC	**Acceso seguro.** Gestionas las credenciales de acceso de los empleados forzando el uso de contraseñas robustas y su cambio periódico, además de incluir el doble factor de autenticación siempre que sea posible.	☐
A	TEC	**Configuración de los dispositivos de teletrabajo.** Configuras los dispositivos utilizados por el empleado para teletrabajar (sistema operativo, antivirus, control de actualizaciones, etc.), tanto si son corporativos como si son aportados por el trabajador (BYOD).	☐
A	TEC	**Cifrado de los soportes de información.** Implantas tecnologías de cifrado que protegen la información de posibles accesos malintencionados.	☐
B	TEC	**Definición de la política de almacenamiento en los equipos de trabajo y en la red corporativa.** Elaboras las políticas que detallan a los empleados dónde deben guardar la información con la que trabajan en remoto.	☐
A	TEC	**Planificación de las copias de seguridad de todos los soportes.** Compruebas regularmente que se realizan periódicamente y que pueden restaurarse.	☐
A	TEC	**Uso de conexiones seguras a través de una red privada virtual o VPN.** Implementas una red VPN extremo a extremo que permite que la información que se intercambia entre los equipos de la organización viaje cifrada a través de Internet.	☐
A	TEC	**Aplicaciones de escritorio remoto siempre a través de una VPN.** Para ofrecer un extra de seguridad y privacidad a las comunicaciones, solo permites el uso de las aplicaciones de escritorio remoto bajo una VPN.	☐
A	TEC	**Virtualización de entornos de trabajo.** Valoras la implementación de la virtualización como método para proporcionar a cada empleado su propio espacio de trabajo, eliminando los riesgos asociados al uso de un dispositivo físico.	☐

NIVEL	ALCANCE	CONTROL	
B	PER	**Priorizar el uso de dispositivos corporativos.** Eliges los dispositivos corporativos para teletrabajar, ya que cuentan con las políticas de seguridad que la empresa considera necesarias y tienen instalado el *software* preciso para realizar el trabajo de forma segura.	☐
B	PER	**Conexión a Internet.** Cuando no es posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utilizas la red de datos móvil 4G o 5G siempre evitando la conexión a redes wifi públicas.	☐
B	PER	**Uso de dispositivos personales bajo una política BYOD.** Utilizas las configuraciones y conexiones permitidas y seguras al teletrabajar desde tus dispositivos personales.	☐
B	PRO	**Concienciar a los empleados antes de empezar a teletrabajar.** Formas a los empleados en ciberseguridad antes de que comiencen a teletrabajar para que conozcan las políticas y las medidas que se llevaran a cabo en la empresa.	☐
A	PRO	**Cumplimiento LOPDGDD.** Formas a los empleados que manejan datos personales para la protección de los mismos durante el teletrabajo y realizas los cambios en los tratamientos para contemplar estas situaciones.	☐
A	TEC/PER	**Aplicaciones de teleconferencia y colaborativas.** Configuras estas aplicaciones para un uso seguro que permita que se respeten la privacidad y la propiedad intelectual de los participantes.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Normativa de protección del puesto de trabajo remoto.** La empresa debe contar con una normativa específica que recoja todas las medidas necesarias para proteger el puesto de trabajo del teletrajador [1], revisando periódicamente su cumplimiento y modificándola si hubiera cambios que la afecten, como por ejemplo: los dispositivos permitidos, los sistemas instalados o las aplicaciones y programas que se consideran necesarios para desempeñar la labor diaria.
- **Relación de usuarios que disponen de la opción de trabajar en remoto**. Será necesario llevar un control de las personas que, por su perfil [2] dentro de la empresa o las características de su trabajo, tienen la opción de teletrabajar.
- **Procedimientos para la solicitud y autorización del teletrabajo:** la organización redactará un documento donde se contemplen todas las cuestiones relativas al teletrabajo (duración del mismo, dispositivos facilitados, etc.), que será firmado por cada teletrabajador.
- **Periodo de implantación y pruebas:** se precisará valorar diferentes escenarios y configuraciones antes de comenzar a teletrabajar. Una implementación demasiado rápida del teletrabajo, sin valorar los riesgos de seguridad, puede poner en peligro la información confidencial de la empresa.
- **Realizar pruebas de carga en escenarios simulados.** Si existe un volumen considerable de empleados que van a teletrabajar al mismo tiempo, debe valorarse la carga que esto ocasiona en los sistemas internos de la empresa.
- **Aplicaciones y recursos a los que tiene acceso cada usuario.** Cada empleado tendrá acceso solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo de su perfil dentro de la organización. Se detallarán las aplicaciones permitidas [4] así como sus condiciones de uso evitando utilizar programas no controlados por la empresa. En el caso de que el empleado necesitase la instalación y uso de un nuevo *software,* este tendrá que ser previamente aprobado por el departamento informático de la empresa.
- **Acceso seguro**. Para las credenciales de acceso [4] se utilizarán contraseñas robustas y el doble factor de autenticación siempre que sea posible, forzando su cambio periódicamente. El mecanismo de gestión de credenciales puede estar controlado por el departamento informático a través de servicios de directorio LDAP, utilizando implementaciones comerciales, como Windows Active Directory o gratuitas, como OpenLDAP entre otras.
- **Configuración de los dispositivos de teletrabajo.** Los dispositivos utilizados por el empleado para teletrabajar serán previamente configurados por los técnicos de la organización (sistema operativo, antivirus, control de actualizaciones [5], etc.), tanto si son corporativos como si son aportados por el trabajador (BYOD) [6].
- **Cifrado de los soportes de información.** Todos los dispositivos deben almacenar la información cifrada [7], tanto para proteger los datos de la empresa de posibles accesos malintencionados, como para garantizar su confidencialidad e integridad.
- **Definición de la política de almacenamiento en los equipos de trabajo en la red corporativa[8]**. Se dispondrá de políticas que detallen a los empleados dónde deben guardar la información con la que trabajan en remoto [8][9].
- **Planificación de las copias de seguridad de todos los soportes.** Deben ser periódicas y comprobar regularmente que pueden restaurarse [10].
- **Uso de conexiones seguras a través de una red privada virtual o VPN.** La implementación de esta tecnología permite que la información que se

intercambia entre los equipos de la organización viaje cifrada a través de Internet, protegiéndola de posibles accesos malintencionados [11].

- **Aplicaciones de escritorio remoto siempre a través de una VPN.** Habilitar el acceso al escritorio desde Internet no es recomendable, puesto que estas aplicaciones pueden contar con vulnerabilidades o configuraciones inadecuadas. Para ofrecer un extra de seguridad y privacidad a las comunicaciones, se recomienda utilizar siempre el escritorio remoto bajo una VPN. Así cuando se acceda a una cuenta por medio del escritorio remoto, primero se deberá acceder a la VPN, la cual proporcionará el acceso al escritorio remoto, haciendo el sistema más robusto [12].
- **Virtualización de entornos de trabajo.** Este tipo de virtualización [13] permite almacenar en un servidor de la empresa el espacio de trabajo de cada empleado en lugar de hacerlo en cada dispositivo de manera local, eliminando los riesgos asociados al uso de un dispositivo propio.
- **Priorizar el uso de dispositivos corporativos.** Estos dispositivos cuentan con las políticas de seguridad que la empresa considera necesarias y tienen instalado el *software* preciso para realizar el trabajo de forma segura [14].
- **Conexión a Internet.** Cuando no sea posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utiliza la red de datos móvil 4G o 5G siempre evitando la conexión a redes wifi públicas.
- **Uso de dispositivos personales bajo una política BYOD.** En el caso de utilizar dispositivos móviles, esta política debe incluir el uso de aplicaciones de administración remota [15] así como lo contemplado en el punto anterior en cuanto a conexión segura a Internet.
- **Concienciar a los empleados antes de empezar a teletrabajar.** Es imprescindible que los empleados reciban formación en ciberseguridad [16] antes de comenzar a teletrabajar y conozcan las políticas y medidas que se llevarán a cabo en la empresa.
- **Cumplimiento LOPDGDD.** Si se han de tratar datos personales desde ubicaciones distintas de las oficinas de la empresa, se ha de contemplar en el análisis de impacto del tratamiento. Además se ha de formar a los empleados para que se garantice en todo caso la privacidad de las personas conforme a la ley.
- **Aplicaciones de teleconferencia y colaborativas.** El uso de estas aplicaciones ha de estar supervisado por el equipo técnico. Se usarán solo las aplicaciones permitidas y con las configuraciones establecidas que permitan un uso seguro.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Guías – Ciberseguridad en el teletrabajo: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/ciberseguridad-el-teletrabajo-guia-aproximacion-el-empresario

[2]. Incibe – Protege tu empresa – Blog – Recomendaciones para una gestión de identidades eficiente https://www.incibe.es/protege-tu-empresa/blog/recomendaciones-gestion-identidades-eficiente

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

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

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

[6]. Incibe – Protege tu empresa – Guías – Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el

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

[8]. 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

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

[10]. Incibe – Protege tu empresa – Guías – Copias de seguridad: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/copias-seguridad-guia-aproximacion-el-empresario

[11]. Incibe – Protege tu empresa – Blog – Conéctate a tu empresa de forma segura desde cualquier sitio con una VPN https://www.incibe.es/protege-tu-empresa/blog/conectate-tu-empresa-forma-segura-cualquier-sitio-vpn

[12]. Incibe – Protege tu empresa – Blog – ¿Es seguro tu escritorio remoto? https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto

[13]. Incibe – Protege tu empresa – Blog – Sistemas VDI y teletrabajo, la dupla perfecta en tiempos del COVID-19 https://www.incibe.es/protege-tu-empresa/blog/sistemas-vdi-y-teletrabajo-dupla-perfecta-tiempos-del-covid-19

[14]. 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

[15]. Incibe – Protege tu empresa – Blog – Cómo prevenir incidentes en los que intervienen dispositivos móviles https://www.incibe.es/protege-tu-empresa/blog/prevenir-incidentes-los-intervienen-dispositivos-moviles

[16]. Incibe – Protege tu empresa – Formación https://www.incibe.es/protege-tu-empresa/formacion

INSTITUTO NACIONAL DE CIBERSEGURIDAD