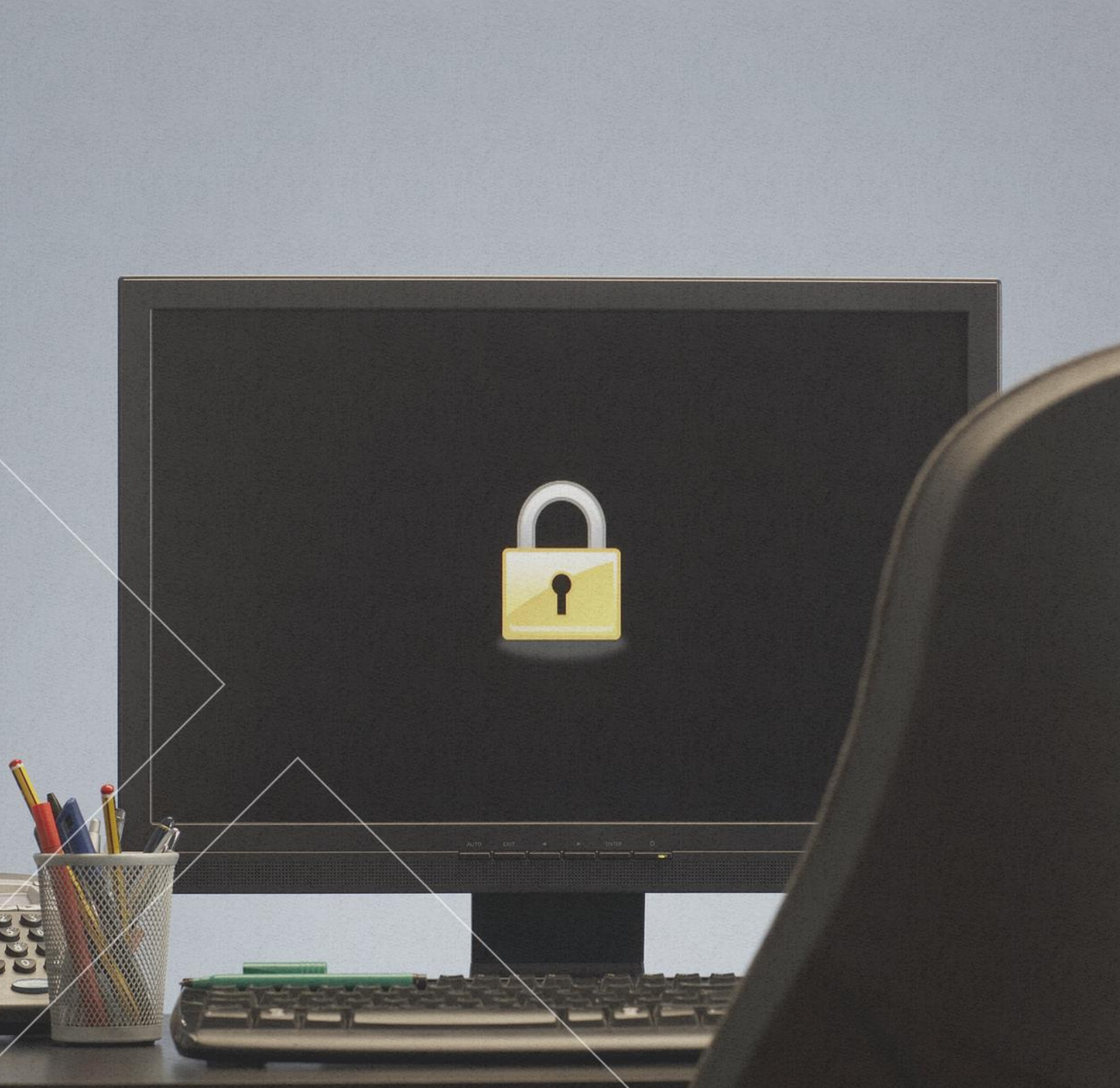

Protección del puesto de trabajo

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. PROTECCIÓN DEL PUESTO DE TRABAJO

1.1. Antecedentes

La gestión de la información empresarial se realiza fundamentalmente desde el puesto de trabajo, tanto desde dispositivos tecnológicos como de forma más tradicional (papel, teléfono,..). De ahí la importancia de concienciar a los empleados y exigir el cumplimiento de ciertas normas para la seguridad en, y desde, su puesto.

Por una parte el empleado debe conocer los riesgos no tecnológicos, por ejemplo:

- información en papel al alcance de personas no autorizadas;
- la falta de confidencialidad de los medios de comunicación tradicionales;
- el peligro de robo o extravío de los dispositivos extraíbles (*pendrives*, discos duros externos, etc.);
- el acceso físico de terceras personas a las zonas de trabajo (repartidores, personal de limpieza, etc.).

Por otra parte desde en muchos puestos de trabajo se tiene acceso a ordenadores, dispositivos móviles y portátiles con conexión a la red de la empresa y al exterior (internet). Son pues una «puerta de entrada» a la empresa y a sus recursos de información. Es esencial preparar a los empleados para evitar incidentes que puedan iniciarse en su puesto de trabajo, acentuados por desconocimiento o por falta de preparación:

- accesos no autorizados a los ordenadores y desde ellos a aplicativos de la empresa;
- infecciones por malware;
- robo y fuga de datos en formato digital;
- ataques de ingeniería social, es decir, engaños para manipular a la víctima para obtener información (credenciales, información confidencial,…) o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso, etc.).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la empresa, debe implantarse una **política de protección del puesto de trabajo**. La organización debe facilitar a los empleados las obligaciones y buenas prácticas en materia de seguridad que apliquen a su puesto de trabajo. Esta normativa debe ser firmada por los empleados en su incorporación a la empresa, así como estar siempre disponible y recordar su aplicación de manera periódica.

1.2. Objetivos

Garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **protección del puesto de trabajo**.

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** Informas al personal sobre la normativa de protección del puesto de trabajo y otra normativa asociada llevando a cabo auditorías periódicas para asegurar su cumplimiento.	☐
A	PRO/TEC	**Destrucción avanzada de documentación mediante mecanismos seguros** Destruyes la información confidencial de forma segura teniendo en cuenta el método apropiado para cada soporte de almacenamiento.	☐
A	TEC	**Bloqueo programado de sesión** Programas un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo.	☐
B	TEC	**Sistema operativo actualizado** Mantienes actualizados los sistemas operativos de los equipos de los usuarios.	☐
B	TEC	**Antivirus actualizado y activo** Mantienes el antivirus actualizado y activo en todos los equipos de los usuarios.	☐
B	TEC	**Deshabilitar por defecto los puertos USB** Deshabilitas por defecto los puertos USB y los habilitas para el personal que necesite dicha funcionalidad.	☐

NIVEL	ALCANCE	CONTROL	
B	TEC	**Seguridad de impresoras y equipos auxiliares** Verificas la seguridad de las impresoras y equipos auxiliares conectados a la red o que puedan almacenar información (cortafuegos, contraseñas,…).	☐
A	PER	**Uso de los medios de almacenamiento** Conoces y aplicas las políticas relativas al almacenamiento seguro de la información.	☐
B	PER	**Prohibición de alteración de la configuración del equipo e instalación de aplicaciones no autorizadas** Solicitas al personal informático la instalación de software específico o el cambio de configuración del equipo si es necesario para el desempeño de tu trabajo.	☐
B	PER	**Política de mesas limpias** Tu mesa de trabajo se encuentra despejada sin documentación confidencial ni dispositivos extraíbles al alcance de otras personas.	☐
B	PER	**Destrucción básica de documentación mediante mecanismos seguros** Utilizas las destructoras de papel para eliminar la información confidencial.	☐
B	PER	**No abandonar documentación sensible en impresoras o escáneres** Recoges inmediatamente aquellos documentos enviados a imprimir y guardas la información una vez escaneada.	☐
B	PER	**No revelar información a usuarios no debidamente identificados** Conoces la existencia y peligros de la ingeniería social y la información que no debes desvelar.	☐
B	PER	**Obligación de confidencialidad** Aceptas y cumples la política de confidencialidad que firmaste al incorporarte al puesto de trabajo.	☐
B	PER	**Uso de contraseñas** No publicas ni compartes tus claves. Tampoco las anotas en documentos ni en cualquier otro tipo de soporte. Usas contraseñas robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,] , ? , etc.) Cambias la contraseña periódicamente.	☐

NIVEL	ALCANCE	CONTROL	
B	PER	**Obligación de bloqueo de sesión y apagado de equipo** Bloqueas la sesión al ausentarte del puesto de trabajo y apagas el equipo al finalizar la jornada laboral.	☐
B	PER	**Uso adecuado de Internet** Conoces y aplicas la normativa relativa al uso de Internet.	☐
B	PER	**Uso de portátiles y dispositivos móviles propiedad de la empresa** Conoces y aceptas la normativa aplicada al uso de portátiles y dispositivos móviles propiedad de la empresa antes de usarlos como herramienta de trabajo.	☐
A	PER	**Cifrado de la información confidencial** Conoces y aplicas la normativa relativa al cifrado de la información.	☐
B	PER	**Obligación de notificar incidentes** Notificas cualquier incidencia de seguridad (virus, pérdida de información o de dispositivos, etc.).	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Normativa de protección del puesto de trabajo.** La empresa debe contar con una normativa específica que recoja todas las medidas necesarias para proteger el puesto de trabajo [1], revisando periódicamente su cumplimiento y modificándola si hubiera cambios que la afecten por ejemplo si se cambian los equipos o los sistemas o se adoptan nuevos servicios.
    - También se dará a conocer a los empleados otras políticas relativas a los equipos o servicios que utilicen en su desempeño: correo electrónico, almacenamiento, etc.
- **Destrucción avanzada de documentación mediante mecanismos seguros.** La información obsoleta se destruirá de forma segura según la Política de borrado seguro y gestión de soportes [2]. En particular:
    - mediante destructoras de papel al servicio de los empleados;
    - contratando un servicio externo de destrucción segura, notificando a los empleados de su existencia y obligación de uso;
    - dando a conocer los riesgos asociados a la utilización de papeleras para documentos sensibles (datos personales, información financiera, etc.).
- **Bloqueo programado de sesión.** El personal informático programará un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo. Adicionalmente se puede contemplar llevar a cabo la programación del apagado general de equipos una vez terminada la actividad empresarial.
- **Sistema operativo actualizado.** El personal responsable de los sistemas aplicará la Política de actualizaciones de software [3] revisando los equipos periódicamente para garantizar su actualización o activando las actualizaciones automáticas.
- **Antivirus actualizado y activo.** El personal responsable de los sistemas aplicará la Política antimalware [13] que incluya la instalación y actualización de herramientas antimalware en todos los equipos y sistemas, y su revisión periódica de manera que se garantice la protección antimalware.
- **Deshabilitar por defecto los puertos USB.** El personal responsable de los sistemas deshabilitará por defecto los puertos USB de todos los equipos y los habilitará para aquellos usuarios que necesiten, de forma justificada y debidamente autorizada, dicha funcionalidad.
- **Seguridad de impresoras y equipos auxiliares de oficina.** El personal responsable verificará que las impresoras [4] y otros equipos conectados a la red o que puedan contener información de la empresa están incluidos en las Políticas de seguridad:
    - estarán dentro del perímetro del cortafuegos;
    - se accederá a su panel de configuración mediante contraseña y por canales cifrados;
    - si tienen wifi se ha de configurar su seguridad;
    - si tienen discos duros se revisarán las Políticas de almacenamiento
    - si tienen conectores USB se deshabilitarán;

    También si fuera posible, se dispondrá de mecanismos de impresión segura (con contraseña) en las impresoras.

- **Uso de los medios de almacenamiento.** Para que el empleado haga un uso correcto de los dispositivos de almacenamiento disponibles, debe conocer y aplicar la normativa corporativa relativa al almacenamiento local en el equipo de trabajo [5], almacenamiento en la red corporativa [6], en la nube [7] y en los dispositivos extraíbles [8].
- **Prohibición de alteración de la configuración del equipo e instalación de aplicaciones no autorizadas.** Es un riesgo que el empleado cambie la configuración del equipo o instale las aplicaciones que considere necesarias. Esta modificación podría tener consecuencias de infección de equipos y por lo tanto de pérdida de información. Si el empleado requiere una configuración o software específico para el desempeño de su trabajo, deberá solicitarlo formalmente al equipo informático.
- **Política de mesas limpias.** Conocemos como política de mesas limpias la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral. No se debe dejar información sensible a la vista de personas que pudieran hacer un uso indebido de la misma. El cumplimiento de esta política conlleva:
    - mantener el puesto de trabajo limpio y ordenado;
    - guardar la documentación y los dispositivos extraíbles que no están siendo usados en ese momento, y especialmente al ausentarnos del puesto o al fin de la jornada laboral;
    - no apuntar usuarios ni contraseñas en post-it o similares.
- **Destrucción básica de documentación mediante mecanismos seguros.** Todo el personal debe utilizar las destructoras de papel para eliminar la información confidencial.
- **No abandonar documentación sensible en impresoras o escáneres.** Para evitar que la información acabe en manos no deseadas el usuario debe:
    - recoger inmediatamente aquellos documentos enviados a imprimir;
    - guardar la documentación una vez escaneada;
    - utilizar los mecanismos de impresión segura si los hubiera.
- **No revelar información a usuarios no debidamente identificados.** La información es uno de los activos empresariales más cotizados. Por este motivo es posible que alguien intente obtener parte de esta información (contraseñas de usuario, información de cuentas bancarias, etc.) engañando a un empleado. Esta práctica se conoce como ingeniería social [9].
  Los delincuentes se hacen pasar por algún responsable, persona o empresa conocida para que el empleado se confíe y facilite la información que le solicitan empleando para ello una llamada telefónica, el correo electrónico, las redes sociales o mensajes del tipo SMS o Whatsapp.
- **Obligación de confidencialidad.** El empleado debe aceptar un compromiso de confidencialidad relativo a cualquier información a la que tenga acceso durante su participación laboral en la empresa. La obligación de confidencialidad tendrá validez todo el tiempo que se haya exigido en el contrato laboral. La información debe protegerse aun cuando el empleado ya no forma parte de la empresa.
- **Uso de las contraseñas.** El usuario debe seguir la Política de contraseñas [10]:
    - las credenciales (usuario y contraseña) son confidenciales y no pueden ser publicadas ni compartidas;

  - no deben anotarse las credenciales en documentos ni en cualquier otro tipo de soporte;
  - las contraseñas deben ser robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,], ?, etc.);
  - se deben cambiar periódicamente.

- **Obligación de bloqueo de sesión y apagado de equipo.** Para evitar el acceso indebido o por personal no autorizado al equipo del puesto de trabajo:
  - el empleado deberá bloquearlo cada vez que se ausente de su puesto;
  - el empleado apagará su equipo al finalizar la jornada laboral.
- **Uso adecuado de Internet .** El empleado debe conocer, aceptar y aplicar la normativa que regula el uso de Internet como herramienta de trabajo con los usos permitidos y prohibidos. También seguirá las recomendaciones de seguridad relativas a la navegación por internet como:
  - verificar que las direcciones (URL) de destino son correctas;
  - verificar que el certificado es válido, cuando se trate de conexiones a entornos seguros (webmail, extranet, etc.) o realicemos transacciones;
  - comprobar que se cumple el protocolo https:// en las páginas donde trabajemos con información crítica.
- **Uso de portátiles y dispositivos móviles propiedad de la empresa.** El empleado debe conocer, aceptar (con su firma) y aplicar la Política de uso de dispositivos móviles [11] de la empresa.
- **Cifrado de la información confidencial.** El empleado debe conocer, aceptar (con su firma) y aplicar la Política de uso de tecnologías criptográficas [12] y la Política de clasificación de información [14] que indica qué información debe ser cifrada.
- **Obligación de notificar incidentes de seguridad.** El empleado debe advertir de cualquier incidente relacionado con su puesto de trabajo:
  - alertas de virus/malware generadas por el antivirus;
  - llamadas sospechosas recibidas pidiendo información sensible;
  - correos electrónicos que contengan virus;
  - pérdida de dispositivos móviles (portátiles, *smartphones* o tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.);
  - borrado accidental de información;
  - alteración accidental de datos o registros en las aplicaciones con información crítica;
  - comportamientos anómalos de los sistemas de información;
  - hallazgo de información en ubicaciones no designadas para ello;
  - evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes,…);
  - evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros;
  - cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protección del puesto de trabajo. https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-puesto-trabajo

[2]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Borrado seguro y gestión de soportes https://www.incibe.es/protege-tu-empresa/herramientas/politicas

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

[4]. Incibe – Protege tu empresa – Blog – ¿Sabías que hasta las impresoras necesitan medidas de seguridad? · https://www.incibe.es/protege-tu-empresa/blog/sabias-las-impresoras-necesitan-medidas-ciberseguridad

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

[6]. 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

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

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

[9]. Incibe – Protege tu empresa – Blog – ¿Cómo combatir la ingeniería social? Este empresario nos lo cuenta · https://www.incibe.es/protege-tu-empresa/blog/combatir-ingenieria-social-este-empresario-nos-cuenta

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

[11]. 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

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

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

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

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD