USO DEL CORREO ELECTRÓNICO

POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

PROTEGE TU EMPRESA

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. USO DEL CORREO ELECTRÓNICO

1.1 ANTECEDENTES

El **correo electrónico** [1] es una herramienta de comunicación imprescindible para el funcionamiento de una empresa. Sus beneficios son evidentes: accesibilidad, rapidez, posibilidad de enviar documentos adjuntos, etc., aunque cuando se creó, no se hizo pensando en sus aplicaciones actuales ni en la seguridad.

Como toda herramienta de comunicación corporativa es necesario definir su uso correcto y seguro, ya que, además de abusos y errores no intencionados en su uso que puedan causar perjuicio en la empresa, el **correo electrónico** se ha convertido en uno de los medios que utilizan los ciberdelincuentes para llevar a cabo sus ataques.

Los empleados pueden incurrir en malas prácticas, como el envío accidental de información a destinatarios incorrectos, filtraciones derivadas de no emplear adecuadamente las opciones de privacidad, manejo inadecuado de archivos adjuntos, envío de informaciones sensibles sin cifrar, usos personales u otras acciones comprometedoras para la empresa.

También es habitual que a los buzones corporativos llegue ***spam***, es decir, comunicaciones no deseadas o correos de *phishing* [2] que suplantan a entidades o a personas. En estos casos, utilizan técnicas de ingeniería social [3] para conseguir sus fines maliciosos, por ejemplo: infectarnos, robar credenciales o que les facilitemos información confidencial. En un correo malicioso, tanto el remitente como el asunto, el cuerpo, los adjuntos o los enlaces que contiene, pueden estar diseñados para engañar al receptor del mensaje. Para impedir caer en la trampa de los ciberdelincuentes, debemos, además de utilizar medios tecnológicos (antivirus, *antimalware*, *antispam*, etc.), concienciar a nuestros empleados para que sepan distinguir estos mensajes [4].

Para evitar los riesgos que conlleva el uso del correo corporativo tenemos que concienciar a nuestros empleados para que hagan un **uso seguro** del mismo e informarles de las normas que regulan las condiciones y circunstancias en las que puede utilizarse, así como las posibles sanciones y acciones a tomar en caso de detectarse un mal uso.

1.2 OBJETIVOS

Establecer unas normas de uso permitido y seguro del correo electrónico corporativo que sirva para impedir errores, incidentes, usos ilícitos y para evitar ataques por esta vía.

1.3 CHECKLIST

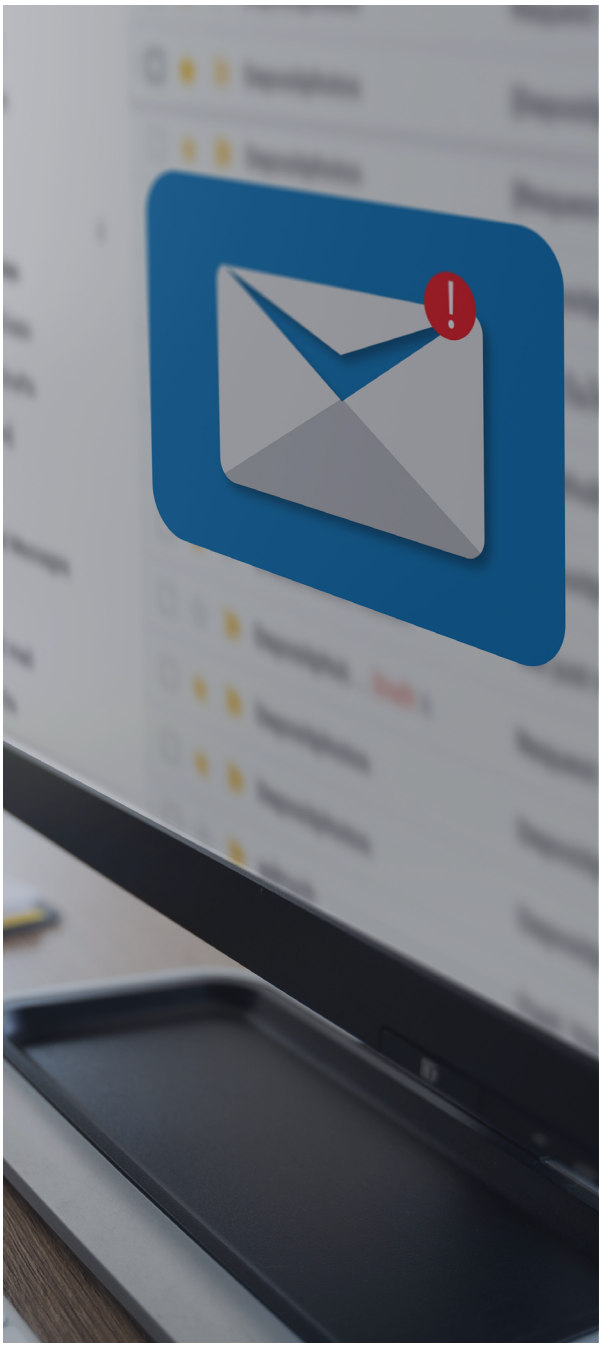
A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al uso del **correo electrónico**.

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.



1.3 CHECKLIST

Nivel	Alcance	Control	
B	PRO	**Normativa de uso de correo electrónico.** Dispones de una normativa referente al uso del correo electrónico que el empleado aceptará al incorporase a su puesto de trabajo.	☐
B	TEC	***Antimalware* y *antispam*.** Instalas y activas aplicaciones *antimalware* y filtros *antispam* tanto en el servidor como en los clientes de correo. Importante mantenerlas actualizadas.	☐
A	TEC	**Cifrado y firma digital.** Instalas una tecnología de cifrado y firma digital que se pueda usar con el correo electrónico para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.	☐
A	TEC	**Desactivar el formato HTML, la ejecución de macros y la descarga de imágenes en los gestores de correo electrónico.** Desactivas el formato HTML, la ejecución de macros y la descarga de imágenes para una protección adicional de las cuentas de correo electrónico.	☐
B	TEC/PER	**Ofuscar las direcciones de correo electrónico.** No publicas las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación.	☐
B	PER	**Uso apropiado del correo corporativo.** Nunca usas el correo corporativo con fines personales y el contenido cumple las normas marcadas por la empresa.	☐
B	PER	**Uso adecuado y racional.** Utilizas el correo electrónico corporativo solo para uso profesional, cumpliendo las reglas de buena fe y diligencia.	☐
B	PER	**Cadenas de mensajes.** Evitas contestar a cadenas de mensajes innecesarias evitando la propagación de correo *spam* o malicioso.	☐
B	PER	**Evitar usos indebidos.** Usas el correo electrónico de manera exclusiva para el ámbito profesional y no haces difusión de material ofensivo o ilegal.	☐
B	PER	**Prestar atención al lenguaje empleado.** Haces uso de lenguaje riguroso, exento de faltas de ortografía.	☐
B	PER	**Vigilar la inscripción en sitios web.** No utilizas el correo electrónico corporativo para registros en páginas web poco confiables o sospechosas.	☐
B	PER	**Contraseña segura.** Usas una contraseña robusta para acceder al correo electrónico.	☐

1.3 CHECKLIST

Nivel	Alcance	Control	
B	PER	**Correos sospechosos.** Sospechas de la autenticidad del correo cuando el mensaje: presenta cambios de aspecto, contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual o solicita credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.)..	☐
B	PER	**Identificación del remitente.** Identificas los remitentes antes de abrir un correo electrónico. Si tienes dudas o sospechas que ha sido suplantado, contactas con el remitente por otro medio para confirmarlo.	☐
B	PER	**Análisis de adjuntos.** Analizas cuidadosamente los adjuntos de correos de remitentes desconocidos antes de abrirlos. Si sospechas de su autenticidad, no lo abres ni lo descargas.	☐
B	PER	**Inspección de enlaces.** Examinas atentamente los enlaces incluidos en los correos antes de acceder a ellos.	☐
B	PER	**No responder al *spam* (correo basura).** Nunca respondes al correo basura. Lo agregas a la lista de *spam* o correo no deseado y lo eliminas.	☐
B	PER	**Utilizar la copia oculta (BCC o CCO).** Utilizas la copia oculta cuando envías correos a múltiples direcciones.	☐
B	PER	**Reenvío de correos.** En caso de necesitar el reenvío de algún correo corporativo a una cuenta personal lo solicitas previamente a la dirección.	☐
B	PER	**Evitar las redes públicas.** No consultas el correo corporativo si estás conectado a redes públicas como wifis de hoteles o aeropuertos.	☐
B	PER	**Acceso a correo electrónico a través de teléfonos móviles corporativos.** No accedes al correo corporativo desde teléfonos móviles que no estén aprobados y configurados por la empresa.	☐
B	PER	**Acceso a correo electrónico a través de clientes web.** No accedes al correo corporativo a través de clientes web desde equipos públicos o compartidos.	☐
B	PER	**Almacenamiento y eliminación del correo electrónico.** Evitas la acumulación innecesaria y no almacenas correos electrónicos corporativos indefinidamente.	☐

Revisado por: _____ **Fecha:** _____

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

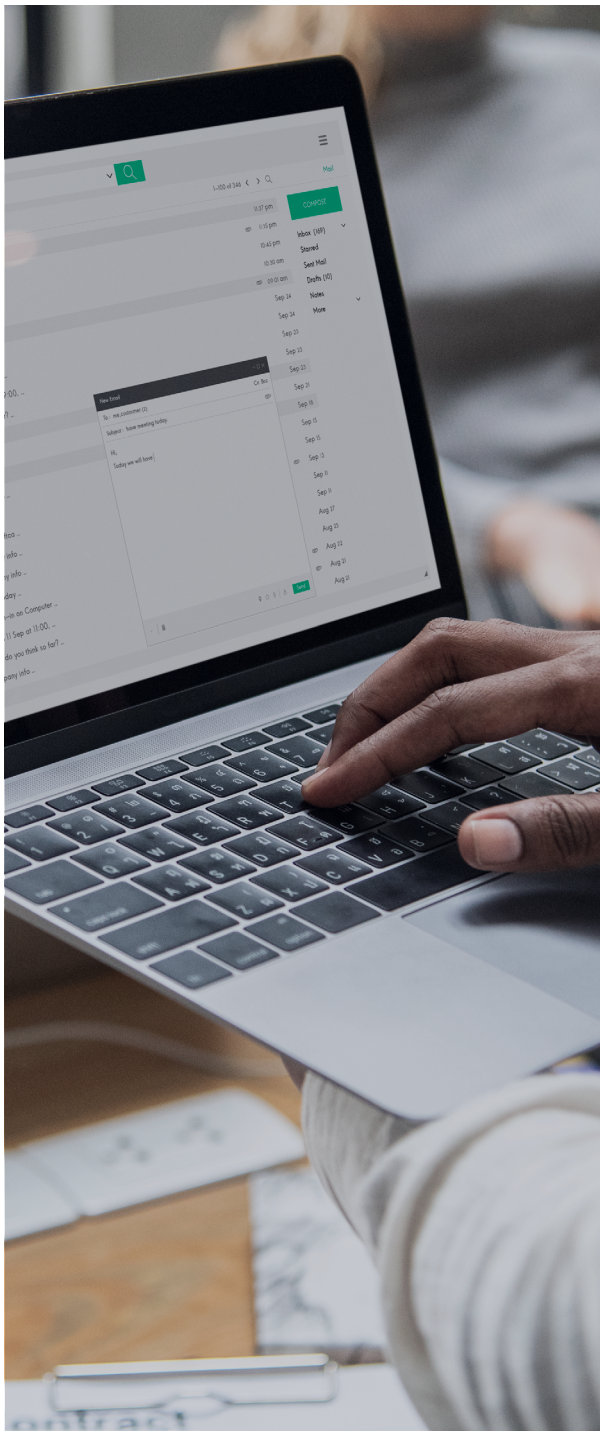
protege tu empresa

1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Normativa de uso de correo electrónico.** La empresa dispondrá de una normativa referente al uso del correo electrónico que el empleado aceptará al incorporase a su puesto de trabajo. Se informará de la prohibición del uso del correo corporativo con fines personales que no tengan que ver con la empresa. El contenido del correo deberá cumplir con la normativa y su uso inadecuado podrá conllevar sanciones.
- ***Antimalware y antispam***. Debes instalar aplicaciones *antimalware* y activar los filtros *antispam* tanto en el servidor como en el cliente de correo según la Política *Antimalware* **[5]**. Estos filtros permitirán que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada evitando así su posible apertura. Se deben mantener estas aplicaciones actualizadas.
- **Cifrado y firma digital**. Se debe instalar una tecnología de cifrado **[6]** y firma digital para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.
- **Desactivar el formato HTML, la ejecución de macros y la descarga de imágenes**. El formato HTML permite utilizar colores, negritas, enlaces, etc. También permite incluir un lenguaje de programación denominado JavaScript. Este lenguaje puede ser usado con fines ilícitos, por ejemplo, para verificar que nuestra cuenta de correo es válida o para redirigirnos a un sitio web malicioso. Por ello es más seguro tenerlo desactivado. Como seguridad complementaria también se deberían deshabilitar las macros y las descargas automáticas de imágenes.

1.4 PUNTOS CLAVE



- **Ofuscar las direcciones de correo electrónico.** No se deben publicar las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación. De lo contrario esas cuentas pueden ser captadas para incluirlas en listas de envío de *spam*. Técnicas que puedes utilizar:
  - Crea una imagen con la dirección de correo que quieras publicar y utiliza la imagen en lugar de introducir el correo como texto.
  - Reemplazar '@' y '.' por texto; de esta forma, nombre@miempresa.com se sustituiría por nombrearrobamiempresapuntocom.
- **Uso apropiado del correo corporativo**. El empleado conoce y acepta la normativa relativa al uso del correo corporativo con fines exclusivamente profesionales.
- **Uso adecuado y racional**. Los empleados deben utilizar el correo electrónico en la medida en que resulte necesario para cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia.
- **Cadenas de mensajes**. No se debe contestar a cadenas susceptibles de provocar congestiones en la bandeja de entrada de mensajes, propagación de correos no deseados o maliciosos o introducir *malware*.

1.4 PUNTOS CLAVE

- **Evitar usos indebidos.** Ningún empleado deberá hacer uso del correo corporativo con fines lucrativos y/o recreativos, de la misma forma que no lo deberá emplear para crear, distribuir o acceder a ninguna clase de material ofensivo o ilegal.
- **Prestar atención al lenguaje empleado.** Normalmente, las comunicaciones que se realicen en el contexto empresarial emplearán un lenguaje riguroso y exento de faltas de ortografía y/o concordancia, ya que cada una de ellas compromete la imagen y el nombre de la empresa. Además, se debe desconfiar de cualquier comunicación supuestamente legítima que emplee un tono informal, carente de sentido o que contenga faltas.
- **Vigilar la inscripción en sitios web.** No se debe emplear el correo corporativo para registros en páginas web que sean poco fiables, de mala reputación o sospechosas de ser ilegales.
- **Ofuscar las direcciones de correo electrónico.** Todas las cuentas deben utilizar contraseñas robustas **[7]** de acceso de acuerdo con la Política de contraseñas **[8]**, se recomienda:
  - Usar una contraseña segura para evitar accesos no autorizados.
  - Utilizar doble factor de autenticación para las cuentas críticas.
  - Si se accede al correo a través desde una interfaz web nunca se marcará la opción de recordar contraseña.
  - Proteger de forma conveniente la contraseña corporativa, no cedérsela a ningún tercero y no utilizarla para realizar ninguna actividad ajena al trabajo.
- **Correos sospechosos.** Los empleados deben aprender a identificar correos fraudulentos y sospechar cuando:
  - El cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente.
  - El mensaje contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual.
  - Se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).
- **Identificación del remitente.** El empleado no abrirá un correo sin identificar el remitente. Si el remitente no es un contacto conocido, habrá que prestar especial atención ya que puede tratarse de un nuevo cliente o de un correo malicioso. Si el remitente es un contacto conocido, pero por otros motivos (cuerpo del mensaje, archivos adjuntos, enlaces...) sospechas que se ha podido suplantar su identidad, debes contactar con éste por otro medio para confirmar su identidad/legitimidad.

1.4 PUNTOS CLAVE

- **Análisis de adjuntos**. Por defecto, no abrir ningún fichero adjunto que no se espera recibir, ni entrar en ningún enlace contenido en el mensaje. Cuando haya que abrirlo, se debe analizar cuidadosamente. Aunque el remitente sea conocido, puede haber sido suplantado y no apercibirnos. La descarga de adjuntos maliciosos podría infectar nuestros equipos con algún tipo de *malware* **[9]**. Tener el antivirus activo y actualizado puede ayudarnos a identificar los archivos maliciosos. Estas son algunas medidas para identificar un adjunto malicioso:
  - Tiene un nombre que nos incita a descargarlo, por ser habitual o porque creemos que tiene un contenido atractivo.
  - El icono no corresponde con el tipo de archivo (su extensión), se suelen ocultar ficheros ejecutables bajo iconos de aplicaciones como Word, PDF, Excel, etc.
  - Tiene una extensión familiar, pero en realidad, está seguida de muchos espacios para que no veamos la extensión real (ejecutable) en nuestro explorador de ficheros, por ejemplo: listadoanual.pdf.exe.
  - Nos pide habilitar opciones deshabilitadas por defecto como el uso de macros.
  - No reconoces la extensión del adjunto y puede que se trate de un archivo ejecutable (hay muchas extensiones con las que no estamos familiarizados).
  - Es o encubre un archivo JavaScript (archivos con extensión .js).
- **Inspección de enlaces.** Al recibir un mensaje con un enlace, antes de hacer clic el receptor debe:
  - **Revisar la URL**, sitúate sobre el texto del enlace, para visualizar la dirección antes de hacer clic en él.
  - **Identificar** enlaces sospechosos que se parecen a enlaces legítimos fijándonos en que:
    - Pueden tener letras o caracteres de más o de menos y pasarnos desapercibidas.
    - Podrían estar utilizando homógrafos, es decir caracteres que se parecen entres sí en determinadas tipografías (1 y l, O y 0).

1.4 PUNTOS CLAVE

- **No responder al *spam* (correo basura).** Cuando recibimos correo no deseado no respondemos al mismo. De lo contrario confirmaremos que la cuenta está activa y seremos foco de futuros ataques. Agrégalo a tu lista de spam y elimínalo. Tampoco lo reenviaremos en caso de cadenas de mensajes.
- **Utilizar la copia oculta (BCC o CCO).** Cuando se envíen mensajes a múltiples destinatarios, envíatelo a ti mismo y utiliza la opción de copia oculta, (CCO o BCO en la mayoría de los clientes de correo) en lugar de la copia normal CC. La copia oculta impide que los destinatarios vean a quién más ha sido enviado. De esta forma evitaremos que cualquiera pueda hacerse con unas cuantas direcciones de correo válidas a las que enviar *spam* o mensajes fraudulentos. Recuerda que el correo electrónico es un dato personal de nuestros clientes y usuarios, que no debemos utilizar para otros fines distintos de aquellos para los que fue solicitado. No debemos divulgarlo o comunicarlo a terceros sin su consentimiento.
- **Reenvío de correos.** Se informará de la prohibición del reenvío de correos corporativos a cuentas personales salvo casos excepcionales que deben ser autorizados por la dirección.
- **Evitar las redes públicas.** Evitar utilizar el correo electrónico desde conexiones públicas (la wifi de una cafetería, el ordenador de un hotel, etc.) de acuerdo con la Política de uso de wifis y conexiones externas **[10]** ya que nuestro tráfico de datos puede ser interceptado por cualquier usuario de esta red. Como alternativa, es preferible utilizar redes de telefonía móvil como el 3G o 4G, estableciendo, a ser posible, conexión de red privada virtual (VPN) **[11]**.
- **Acceso a correo electrónico a través de teléfonos móviles corporativos.** Los empleados solo accederán al correo electrónico corporativo desde los dispositivos móviles que sean autorizados por la empresa, evitando el uso desde dispositivos personales.
- **Acceso a correo electrónico y a través de cliente web.** Los empleados garantizarán que no harán uso de dispositivos públicos o compartidos para acceder al correo electrónico corporativo.
- **Almacenamiento y eliminación del correo electrónico.** Es responsabilidad de los trabajadores realizar un mantenimiento de las cuentas de correo electrónico, evitando la acumulación y almacenamiento innecesarios.

2. REFERENCIAS

[1] INCIBE – Empresas – Blog – Consejos para hacer un uso seguro del correo corporativo https://www.incibe.es/empresas/blog/consejos-hacer-uso-seguro-del-correo-corporativo

[2] INCIBE – Empresas – TemáTICas – Phishing – https://www.incibe.es/empresas/tematicas/phishing

[3] INCIBE – Empresas- TemáTICas – Ingeniería Social – https://www.incibe.es/empresas/tematicas/ingenieria-social

[4] INCIBE – Empresas – Blog – Luchando contra la ingeniería social: el firewall humano- https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

[5] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Antimalware https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/antimalware.pdf

[6] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Uso de técnicas criptográficas – https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

[7] INCIBE – Empresas – Blog – Los riesgos y las medidas de seguridad del correo electrónico https://www.incibe.es/empresas/blog/los-riesgos-y-las-medidas-seguridad-del-correo-electronico

[8] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Contraseñas https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

[9] INCIBE – Empresas – TemáTICas – Malware – https://www.incibe.es/empresas/tematicas/malware

[10] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Uso de wifis y redes externas – https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-wifis-y-redes-externas.pdf

[11] INCIBE – Empresas - Blog – Recomendaciones de seguridad en el empleo de redes VPN – https://www.incibe.es/empresas/blog/recomendaciones-seguridad-el-empleo-redes-vpn

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

INSTITUTO NACIONAL DE CIBERSEGURIDAD