CONTRASEÑAS

POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

PROTEGE TU EMPRESA

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. CONTRASEÑAS

1.1 ANTECEDENTES

El tratamiento diario de la información de la empresa requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos la pareja de credenciales: **usuario y contraseña**. Por la seguridad de los servicios y sistemas en los que existen cuentas de usuarios, tenemos que garantizar la que las **credenciales de autenticación** se generan, actualizan y revocan de forma óptima y segura.

Existen distintos mecanismos de **gestión de identidades y control de accesos**. Algunos, están implementados en los sistemas operativos habituales, otros, están disponibles a través de servicios *online* como pueden ser el ***social login***, la federación de identidades, los servicios de intermediarios de seguridad de acceso a la nube o CSAB, etc. En cualquier caso, debemos establecer un **procedimiento claro para habilitar y revocar las credenciales y permisos de acceso** [1] a los distintos servicios y aplicaciones: correo electrónico, servidor de ficheros, gestor de contenidos web, CRM, ERP, etc.

En el control de accesos, el nombre de usuario nos identifica y la contraseña nos autentica (con ella se comprueba que somos quienes decimos ser). Todo sistema de autenticación [2] [3] de usuarios se basa en la utilización de uno, o varios, de los siguientes factores:

- **algo que sabes:** contraseñas, preguntas personales, etc.
- **algo que eres:** huellas digitales, iris o retina, voz, etc.
- **algo que tienes:** *tokens* criptográficos, tarjeta de coordenadas, etc.

Como la contraseña es el más utilizado de estos factores, la **gestión de las contraseñas** es uno de los aspectos más importantes para asegurar nuestros sistemas de información. Las contraseñas débiles o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos y servicios de nuestra empresa.

Dentro de la gestión de contraseñas se incluye el deber de difundir y hacer cumplir unas buenas prácticas: actualizarlas periódicamente, garantizar su fortaleza (dificultad para adivinarla o craquearla), no utilizar contraseñas por defecto y cómo custodiarlas.

1.2 OBJETIVOS

Establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de **contraseñas**.

1.3 CHECKLIST

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

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	
A	PRO/TEC	**Gestión de contraseñas.** Defines un sistema de gestión de contraseñas avanzado que contempla todos los aspectos relativos a su ciclo de vida.	☐
A	PRO/TEC	**Técnicas de autenticación externas.** Consideras la utilización de sistemas de autenticación externos descentralizados.	☐
A	TEC	**Herramientas para garantizar la seguridad de las contraseñas.** Te ayudas de técnicas y herramientas informáticas para garantizar la seguridad de las contraseñas.	☐
B	TEC	**No utilizar las contraseñas por defecto.** Cambias las contraseñas que vienen incluidas por defecto para el acceso a aplicaciones y sistemas.	☐
B	TEC	**Doble factor de autenticación (2FA).** Incorporar sistemas de autenticación multifactor en los accesos a servicios siempre que sea posible. Es una capa de seguridad extra.	☐
B	PER	**No compartir las contraseñas con nadie.** Mantienes en secreto tus claves y evitas compartirlas.	☐
B	PER	**Las contraseñas deben de ser robustas.** Generas tus contraseñas teniendo en cuenta su fortaleza.	☐
B	PER	**No utilizar la misma contraseña para servicios diferentes.** Te aseguras de elegir distintas contraseñas para cada uno de los servicios que utilizas.	☐
B	PER	**Cambiar las contraseñas periódicamente.** Haces que se modifiquen las contraseñas cada _____.	☐
B	PER	**No hacer uso del recordatorio de contraseñas.** No utilizas nunca las opciones de recordatorio de contraseñas de navegadores y aplicaciones.	☐
B	PER	**Utilizar gestores de contraseñas.** Usas gestores de contraseñas seguros para poderlas recordar.	☐
B	PER	**Ciberllave o Passkey.** Asegurar la información con el uso de ciberllave o passkey en las plataformas que lo permitan.	☐

Revisado por: _____ **Fecha:** _____

1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Gestión de contraseñas.** La gestión de contraseñas es uno de los aspectos más delicados para asegurar el acceso a nuestros sistemas. Se ocupa de:
  - **Identificar** los distintos equipos, servicios y aplicativos para los que es necesario activar credenciales de acceso.
  - **Definir** la manera con la que se generarán las **claves**, así como su formato.
  - **Distribuir** las claves generadas a los usuarios correspondientes, teniendo en cuenta: si esta distribución ha de ser cifrada y con qué método; cómo se activarán las claves.
  - **Almacenar** las claves en repositorios seguros, considerando la necesidad de realizar copias de respaldo **[4]**.
  - **Determinar** quién puede acceder a estos repositorios y cómo.
  - **Establecer** el periodo de validez para cada tipo de clave.
  - **Revocar** las claves, ya sea por baja de un empleado, por considerar que una clave está comprometida por robo, etc. Además, se determinará la manera con la que las claves serán eliminadas.
  - **Registrar**: motivo por el que se genera una clave; fecha de creación; responsable de la custodia; periodo de validez; posibles observaciones, incidentes, etc.

1.4 PUNTOS CLAVE

- **Técnicas de autenticación externas**. Los avances en el mundo digital posibilitan la elección de mecanismos de autenticación descentralizados que permiten el uso de contraseñas únicas para acceder a varios servicios. En ciertos casos, la empresa puede plantarse el uso de alguna de estas técnicas, teniendo siempre en cuenta el riesgo que supone permitir que terceros gestionen nuestras credenciales:
  - ***Social-login***. Se basa en la utilización de identidades, ya creadas en redes sociales (como Facebook, LinkedIn, Google o X), para registrarnos automáticamente en otros servicios.
  - **Autenticación federada**. Permite a los usuarios acceder a múltiples sistemas o servicios a través de una única identidad digital. Se utiliza un sistema centralizado que autentica al usuario y proporciona información de autenticación a los diferentes servicios cuando se necesita. De esta forma, se elimina la necesidad de crear y recordar múltiples credenciales.
  - ***Single-sign-on (SSO)***. Se trata de un sistema de autenticación que permite a los usuarios autenticados acceder a múltiples aplicaciones y servicios vinculados sin necesidad de volver a autenticarse.
  - **Autenticación condicionada al dispositivo**. Evalúa y valida la identidad de un usuario en función de características y propiedades específicas de su dispositivo, como la dirección IP, el tipo de dispositivo, el sistema operativo o la ubicación.
  - **CSAB (*Cloud Access Security Brokers*)**. Especialmente pensado para empresas que hacen uso de servicios *cloud*. Esta herramienta está diseñada para proteger los datos y aplicaciones que se almacenan en entornos de nube. Actúan como intermediarios entre los usuarios y los servicios *cloud*, supervisando el tráfico y garantizando la seguridad, proporcionando una capa adicional de protección y control.
- **Herramientas para garantizar la seguridad de tus contraseñas**. Para garantizar que nuestras contraseñas se generan y usan de forma robusta, podemos ayudarnos de diversas herramientas como LDAP, *Active Directory* o servicios externos que obligan al cumplimiento de ciertos requisitos. En todos los casos se contemplarán los aspectos más relevantes como:
  - **Periodos** de validez para las contraseñas.
  - **Posibilidad** de reutilización de contraseñas ya usadas.
  - **Formato de la contraseña**: longitud mínima; tipos de caracteres que deben incluir; cumplimiento de reglas semánticas.
  - **Posibilidad** de elección y modificación de la contraseña por parte del usuario.
  - **Almacenamiento de las claves**: tamaño del histórico de claves a almacenar para cada usuario; método de encriptación de las claves.
  - **Número de intentos** de autenticación permitidos.

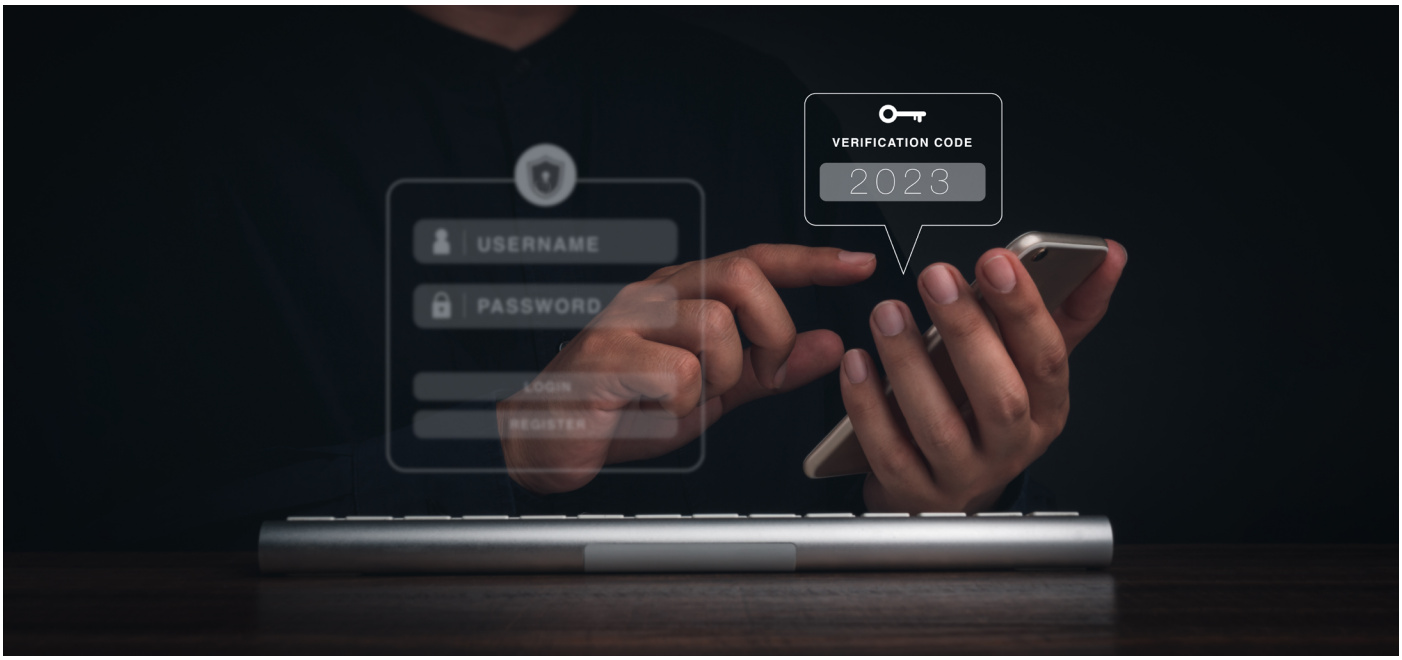
1.4 PUNTOS CLAVE

- **No utilizar las contraseñas por defecto.** Debemos cambiar las claves por defecto, las que traen los equipos y sistemas al adquirirlos, por otras elegidas por nosotros mismos. Con esta medida evitamos el acceso no permitido, que sería posible si dejamos la contraseña por defecto por ser estas conocidas o que pueden encontrarse fácilmente en Internet. Esto es especialmente importante para el acceso a la configuración de ciertos dispositivos como *routers*, *switches*, etc.

- **Doble factor de autenticación (2FA)** [5] [6]. Requiere dos formas diferentes de verificar la identidad de un usuario antes de permitirle acceder a un sistema. Generalmente, implica el uso de dos factores: algo que el usuario sabe, como la contraseña, y algo que el usuario tiene, como un código recibido en su móvil. Este sistema proporciona una capa adicional de seguridad, ya que, en caso de que un ciberdelincuente se hiciese con una de las formas de autenticación, necesitaría la segunda para poder acceder. Algunos **ejemplos de 2FA** son: huella digital; *tokens* criptográficos *hardware*; sistemas *OTP (One Time Password)*; SMS; tarjetas de coordenadas.

- **No compartir las contraseñas con nadie**. Si compartimos nuestras contraseñas dejarán de ser secretas y por tanto perderán su utilidad. Debemos asegurarnos de lo siguiente:

  - **No** debemos compartirlas con nadie.
  - **No** debemos apuntarlas en papeles o *post-it*.
  - **No** debemos escribir nuestras contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.



1.4 PUNTOS CLAVE

- **Las contraseñas deben de ser robustas [7].** Para que nuestras contraseñas sean fuertes, difíciles de adivinar o calcular, debemos cumplir las siguientes directrices:
  - **Deben contener al menos doce caracteres**, pero se recomienda un mínimo de catorce.
  - **Deben combinar caracteres de distinto tipo** (mayúsculas, minúsculas, números y símbolos).
  - **No deben contener los siguientes tipos de palabras**: palabras sencillas en cualquier idioma (palabras de diccionarios); nombres propios, fechas, lugares o datos de carácter personal; palabras que estén formadas por caracteres próximos en el teclado; palabras excesivamente cortas.
  - **Tampoco utilizaremos claves formadas** únicamente por elementos o palabras que puedan se públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento).
  - **Se establecerán contraseñas más fuertes** para el acceso a aquellos servicios o aplicaciones más críticas.
  - **Se tendrá en cuenta lo expuesto en los puntos anteriores** también en el caso de utilizar contraseñas de tipo *passphrase* (contraseña larga formada por una secuencia de palabras).
- **No utilizar la misma contraseña para servicios diferentes**. Nunca debemos utilizar la misma contraseña para diferentes servicios. Tampoco utilizaremos las mismas contraseñas para uso profesional y doméstico. De esta forma evitaremos tener que cambiar todas nuestras contraseñas en el caso de que solo una haya sido comprometida.
- **Cambiar las contraseñas periódicamente [8]**. Para garantizar la confidencialidad de nuestras contraseñas estas deben ser cambiadas periódicamente. La periodicidad dependerá de la criticidad de la información a la que dan acceso. No deben utilizarse contraseñas que hayan sido usadas con anterioridad. Pueden utilizarse sistemas que fuercen al cambio de contraseña en el plazo elegido.
- **No hacer uso del recordatorio de contraseñas**. No es recomendable el utilizar las funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personal no autorizado. Esto es especialmente frecuente en el uso de navegadores web.
- **Utilizar gestores de contraseñas [9]**. Debemos considerar el uso de gestores de contraseñas en aquellos casos en los que tengamos que recordar un gran número de ellas para acceder a muchos servicios. En estos casos es muy recomendable elegir un gestor cuyo control quede bajo nuestra supervisión, que cifre las credenciales e implantar doble factor de autenticación para acceder al mismo.

2. REFERENCIAS

[1] INCIBE – Protege tu empresa – Herramientas – Políticas de seguridad - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf

[2] INCIBE – Protege tu empresa – TemáTICas - TemáTICas Autenticación - https://www.incibe.es/empresas/tematicas/autenticacion

[3] INCIBE – Protege tu empresa – Blog - TemáTICas: autenticación segura, ¿qué es y por dónde empiezo? - https://www.incibe.es/empresas/blog/tematicas-autenticacion-segura-y-donde-empiezo

[4] INCIBE – Protege tu empresa - Herramientas – Políticas de seguridad - Copias de seguridad - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/copias-seguridad.pdf

[5] INCIBE – Protege tu empresa – Blog - Asegura tus cuentas de usuario con la autenticación de doble factor - https://www.incibe.es/empresas/blog/asegura-tus-cuentas-usuario-autenticacion-doble-factor

[6] INCIBE – Protege tu empresa – Blog - Dos mejor que uno: doble factor para acceder a servicios críticos - https://www.incibe.es/empresas/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

[7] INCIBE – Protege tu empresa – Blog - Desempolvando Políticas de seguridad: las contraseñas - https://www.incibe.es/empresas/blog/desempolvando-politicas-seguridad-las-contrasenas

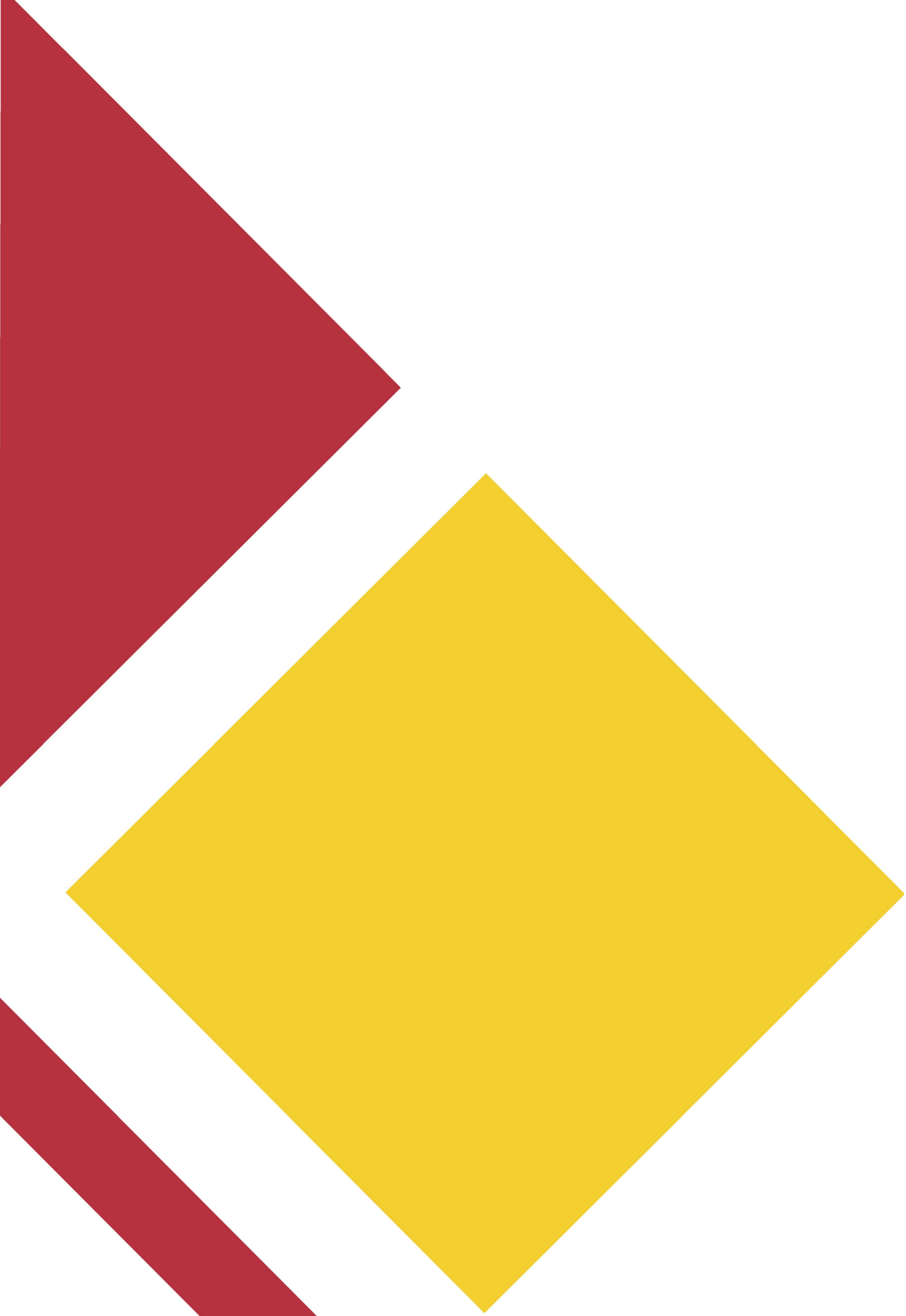
[8] INCIBE – Protege tu empresa – Blog - ¿Cuánto hace que no cambias tus contraseñas? - https://www.incibe.es/empresas/blog/cuanto-hace-no-cambias-tus-contrasenas

[9] INCIBE – Ciudadanía – Blog – Gestores de contraseñas: ¿cómo funcionan? - https://www.incibe.es/ciudadania/blog/gestores-de-contrasenas-como-funcionan

Más información al respecto:

[10] INCIBE - Protege tu empresa – Blog - Celebra el Día Mundial de las Contraseñas, la puerta de entrada a todos tus servicios - https://www.incibe.es/empresas/blog/celebra-el-dia-mundial-las-contrasenas-puerta-entrada-todos-tus-servicios

[11] INCIBE – Protege tu empresa – Blog - Con estos ataques nos roban las contraseñas, ¡aprende a evitarlos! - https://www.incibe.es/empresas/blog/estos-ataques-nos-roban-las-contrasenas-aprende-evitarlos



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

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa