POLÍTICA DE SEGURIDAD DE LAS CONTRASEÑAS

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 [2], 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 [12] 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 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
[1] es uno de los aspectos más importantes para asegurar nuestros sistemas de información. Las contraseñas deficientes 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 o 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.

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 para servicios críticos** Incorporas sistemas de autenticación multifactor en los accesos a servicios con información muy sensible.	☐
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.	☐

NIVEL	ALCANCE	CONTROL	
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 tercer mes.	☐
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.	☐

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
CARGO:	Consultor	Gerencia	Gerencia
NOMBRE:	Ing. Enith E. Gustin	Diego Córdoba	Diego Córdoba
Fecha:	2024-01-27	2024-01-28	2024-02-01

CONTROL DE CAMBIOS		
VERSIÓN No.	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**
1	2024-02-01	Creación del documento