Política de contraseñas

POL-SI-06

Sistemas de la Información

Histórico de versiones

Versión	Fecha	Autor	Validador	Aprobador	Cambios
1.0	Abril 2020	Departamento IT	Departamento IT	Departamento IT	Versión inicial
1.1	Agosto 2020	Departamento IT	Departamento IT	Departamento IT	Revisión y cambios menores

Referencia a otros documentos

- POL-SI-05 - Política de gestión incidentes

Contenido

1 INTRODUCCIÓN

1.1 Objeto y Contenido

Las contraseñas o passwords constituyen el mecanismo básico que se emplea para la autenticación de los usuarios para el acceso a servicios y aplicaciones. La fortaleza del mecanismo de autenticación basado en contraseña se fundamenta en dos principios básicos. En primer lugar, la contraseña debe ser secreta; sólo debe conocerla el propio usuario que además es el responsable de su custodia. En segundo lugar, no debe ser posible averiguar la contraseña; las contraseñas no deben ser predecibles ni deducibles a partir de información disponible de forma pública.

Si alguna de las dos condiciones anteriores no se cumple, se puede comprometer no sólo la seguridad del usuario sino de toda la compañía. Todos los usuarios son responsables de sus contraseñas de acceso a servicios y aplicaciones y de los accesos que se produzcan haciendo uso de esas contraseñas.

1.2 Ámbito de Aplicación

Esta política afecta a cualquier persona o empresa que acceda a la Información de Doctaforum Medical Marketing S.L., en adelante, la Compañía.

Las empresas pertenecientes a Doctaforum Medical Marketing S.L. seguirán las directrices de la Compañía así como los documentos que emanen de éstas.

1.3 Distribución

Una vez aprobado por el Comité, se divulgará a todos los empleados afectados, a través del sistema de gestión documental establecido.

1.4 Entrada en vigor

El presente documento entrará en vigor una vez aprobado formalmente y en la fecha que se indica en su cabecera.

1.5 Revisión del Documento

El presente documento deberá ser revisado con una periodicidad anual, salvo la necesidad de un cambio sobre el mismo.

2 RECOMENDACIONES SOBRE EL USO DE CONTRASEÑAS

- Evitar utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf”, “1234”...).
- No se debe utilizar información personal en la contraseña: nombre del usuario, apellidos, fecha de nacimiento, aniversarios, nombres de familiares, DNI o número de teléfono.
- No emplear las mismas contraseñas utilizadas en cuentas de usuario o accesos relacionados con el entorno laboral para cuentas personales.
- Independientemente del período de caducidad de las contraseñas establecidas en los diferentes sistemas de la compañía, se recomienda no mantener la misma contraseña más de 6 meses.

3 POLÍTICA DE CONTRASEÑAS

Las contraseñas deberán cambiarse como mínimo una vez al año.

Todas las contraseñas deberán contener letras mayúsculas y minúsculas, así como un mínimo de un dígito o símbolo.

Todas las contraseñas deberán tener una longitud mínima de 8 caracteres.

El acceso a cualquier sistema accediendo con las cuentas descritas en este punto, será bloqueado tras un máximo de 5 inicios de sesión fallidos y requerirá que el departamento de sistemas desbloquee la cuenta de forma manual.

Actualmente los empleados de la compañía disponen de 3 cuentas principales para el acceso a los sistemas corporativos.

- **Cuenta de usuario de dominio**. Utilizada para iniciar sesión en el equipo corporativo, acceso a carpetas compartidas del servidor de ficheros (ML350 y NAS) y acceso a la VPN.
- **Cuenta de Office 365**. Utilizada para acceder al correo corporativo, activación de Office en equipos de escritorio, Teams y acceso a recursos de Office desde dispositivos móviles tales como, Company Portal, aplicaciones de ofimática, correo electrónico o Teams.
- **Cuenta de Doctaforum web APP**. Destinada al acceso a la aplicación web de la compañía. Esta requiere el uso de tarjeta de coordenadas proporcionada en el momento de alta en la plataforma.

En el caso de sospecha de acceso no autorizado, el usuario deberá informar a al departamento de sistemas de forma inmediata según el procedimiento descrito en "*POL-SI-05 - Política de gestión incidentes*".