RGPD
LOPDGDD
✓

Seguridad de los datos personales: Política de buenas prácticas en la gestión de contraseñas

Programa de cumplimiento activo de la normativa de protección de datos personales

CUMPLE

audidat
PROTECCIÓN DE DATOS

POLÍTICA DE «BUENAS PRÁCTICAS EN LA GESTIÓN DE CONTRASEÑAS»

I. OBJETO DEL DOCUMENTO

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (en adelante, RGPD), proporciona un marco modernizado y basado en la rendición de cuentas para la protección de los datos en Europa.

En tal sentido, el artículo 5, apartado 2, del Reglamento (UE) 2016/679, establece expresamente el principio de «responsabilidad proactiva», según el cual el responsable del tratamiento será responsable del cumplimiento (y capaz de demostrarlo), entre otros, del principio de «integridad y confidencialidad», según el cual:

> *Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).*

De tal modo, el Considerando 39 del Reglamento (UE) 2016/679 establece lo siguiente:

> *(...) Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.*

A este respecto, interesa subrayar que las contraseñas son el mecanismo de autenticación más generalizado para el acceso a los datos personales y a los equipos utilizados para su tratamiento. En tal sentido, la aprobación, difusión y cumplimiento de una política de buenas prácticas en la gestión de contraseñas, es un aspecto trascendental para garantizar una seguridad y confidencialidad adecuadas de los datos personales objeto de tratamiento y, en particular, para impedir el acceso o uso no autorizados de dichos datos.

En su consecuencia, el objeto del presente documento es establecer una política de «Buenas prácticas en la gestión de contraseñas» en relación con el acceso a los datos personales responsabilidad de la entidad y a los equipos utilizados para su tratamiento.

A tal fin, se han seguido las orientaciones y directrices recogidas en los siguientes documentos:

- Guía de Seguridad de las TIC. CCN-STIC 821. Apéndice V: Normas de Creación y Uso de Contraseñas NP40. Centro Criptológico Nacional (CCN).
- Políticas de seguridad para la pyme: contraseñas. Instituto Nacional de Ciberseguridad (INCIBE).
- Recomendaciones de la Agencia Española de Protección de Datos (AEPD).

II. NORMAS GENERALES DE USO DEL SISTEMA DE INFORMACIÓN

Las presentes «Buenas prácticas en la gestión de contraseñas» complementan, en sus aspectos específicos, a la «Política de uso del sistema de información: Normas de uso del conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto», por lo que las citadas normas generales de uso serán de aplicación en los aspectos no recogidos en este documento.

III. GESTIÓN DE CONTRASEÑAS

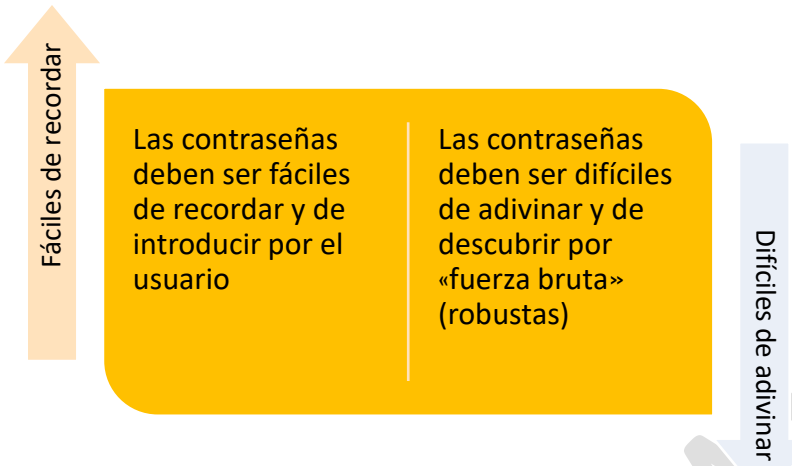
Dentro de una adecuada política de gestión de contraseñas se incluye el deber de garantizar su fortaleza, la corrección en su uso para preservar la confidencialidad de las mismas, su actualización periódica, la difusión de unas buenas prácticas entre los usuarios del sistema de información, así como la realización de controles regulares de cumplimiento de las mismas.

En tal sentido, las presentes «Buenas prácticas en la gestión de contraseñas» se estructuran en los siguientes apartados:

1. CREACIÓN DE CONTRASEÑAS

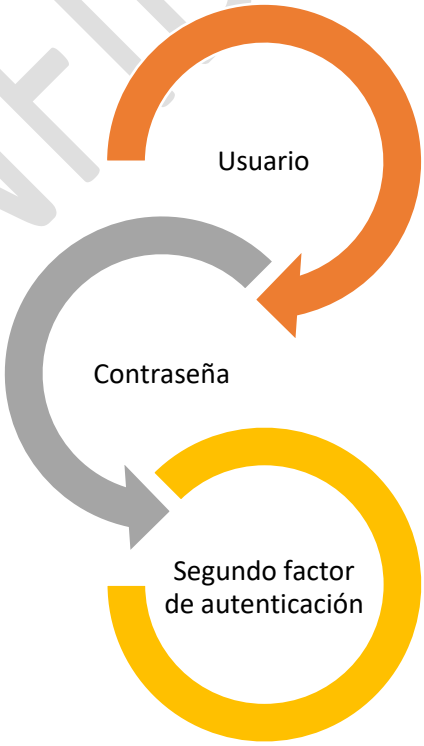
Las contraseñas son, junto al código o identificador de usuario, el medio de acceso a los datos personales y a los equipos utilizados para su tratamiento. De tal modo, para garantizar una seguridad y confidencialidad adecuadas de los datos personales, es necesario que las contraseñas que se utilicen como mecanismo de autenticación para el acceso a los mismos sean «robustas», esto es, difícilmente vulnerables.

En tal sentido, las contraseñas deben ser fáciles de recordar y de introducir por el usuario, y asimismo difíciles de adivinar y de descubrir por «fuerza bruta». El ataque de fuerza bruta es la forma de descubrir una contraseña probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.



En el ámbito de la ciberseguridad, la Agencia Española de Protección de Datos recomienda implementar un «sistema de autenticación de doble factor» para el acceso a la «información crítica»: aquella información que resulta indispensable para el desarrollo de las operaciones intrínsecas a la actividad del responsable del tratamiento.

El uso de un segundo factor de autenticación consiste en añadir una capa de seguridad «extra», de manera que, aparte del código o identificador de usuario y la contraseña, sea preciso un elemento adicional de comprobación para el acceso a la información crítica. Este segundo factor de seguridad puede ser, entre otros, un elemento biométrico (por ejemplo, la huella digital del usuario), un código pseudoaleatorio, o el envío de un código de un solo uso establecido para cada usuario.



a) Las contraseñas deben ser difíciles de adivinar y de descubrir por «fuerza bruta».

Para que las contraseñas sean suficientemente fuertes y difícilmente adivinables por terceros, con carácter general deberán seguirse las siguientes «Directrices generales para la creación de contraseñas robustas»:

Directrices generales para la creación de contraseñas robustas

1. Deberán tener una longitud mínima de 8 caracteres. La longitud deberá ser mayor de 8 caracteres si se trata de una contraseña de acceso a «categorías especiales de datos personales» o a datos muy personales, cuya violación implique graves repercusiones para el interesado (por ejemplo, datos bancarios), limitando el sistema el número de intentos de acceso sin éxito.
2. Deberán combinar caracteres de distinto tipo: letras mayúsculas y minúsculas, números y signos de puntuación. En caso de dificultad del usuario para recordar una contraseña de estas características, podrá utilizarse una contraseña de tipo «passphrase»: una contraseña larga formada por una secuencia de palabras cuya deducción, automática o no, no sea simple.
3. No deberán coincidir con el código o identificador de usuario.
4. No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario: nombre, apellidos, ciudad o fecha de nacimiento, número de DNI, nombres de familiares, matrícula del coche, etc., o combinaciones de las mismas (por ejemplo, nombre + año de nacimiento).
5. No deberán estar basadas en el uso de caracteres repetitivos (por ejemplo, «aaaaaaaa») o secuenciales (por ejemplo, «1234abcd»)
6. No deberán coincidir con palabras sencillas en cualquier idioma que puedan figurar en un diccionario (por ejemplo, «caracola»).
7. No deberán estar basadas en palabras formadas por caracteres próximos en el teclado (por ejemplo, «qwertyui»).
8. No deberán coincidir con frases famosas o refranes, estrofas de canciones o frases impactantes de películas o de obras de literatura.
9. La contraseña no deberá ser igual a ninguna de las últimas contraseñas usadas, ni estar formada por una concatenación de ellas (no reutilización).

b) Las contraseñas deben ser fáciles de recordar y de introducir por el usuario.

Como hemos señalado anteriormente, las contraseñas también deben ser fáciles de recordar por el usuario. En este sentido, un mecanismo útil para recordar una contraseña creada a partir de una combinación de caracteres de distinto tipo, son los llamados «acrósticos», que consisten en seleccionar un carácter de cada palabra de una frase fácilmente memorizable. Por ejemplo, la frase «Mi nombre es Mata Hari. Tengo 41 años.», puede generar la cadena de caracteres «MneMH.T41a.».

Si, no obstante, el usuario sigue teniendo dificultades para recordar su contraseña, existe la amenaza de que la apunte en un papel, pósit, o en cualquier otro lugar no seguro, comprometiendo la confidencialidad de la misma. En dicho caso concreto, se ha de implementar una solución de compromiso entre la robustez de la contraseña y la facilidad con la que el usuario puede recordarla, como utilizar una contraseña de tipo «passphrase»: una contraseña larga formada por una secuencia de palabras cuya deducción, automática o no, no sea simple (por ejemplo, «lapiceronubecoche»). Dicha secuencia de palabras también puede incluir los espacios en blanco (por ejemplo, «lapicero nube coche»). Así mismo, pueden utilizarse frases cortas sin sentido (por ejemplo, «me voy de compras al río»).

2. USO DE CONTRASEÑAS

Para preservar la confidencialidad de las contraseñas, con la finalidad de impedir el acceso o uso no autorizados de los datos personales responsabilidad de la entidad, los usuarios del sistema de información deberán cumplir las siguientes «Directrices generales de uso de contraseñas»:

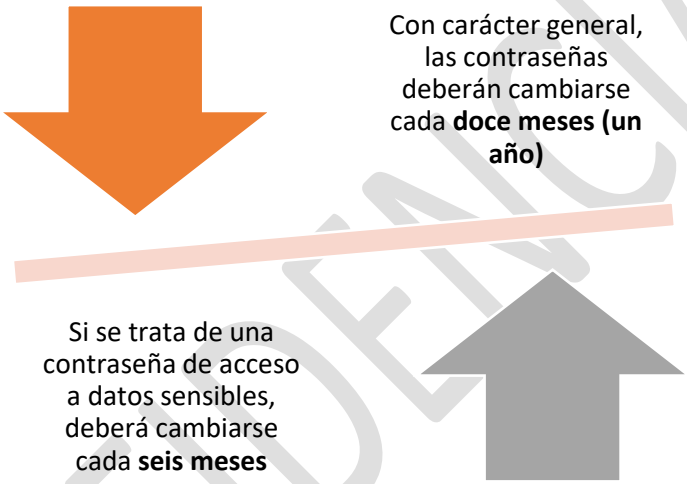
Directrices generales de uso de contraseñas

1. El usuario deberá salvaguardar en todo momento el carácter confidencial, personal e intransferible de la contraseña. No deberá entregarla ni comunicarla a nadie. En caso de haber tenido necesidad de hacerlo por motivos de trabajo o mantenimiento, el usuario deberá proceder a cambiarla de forma inmediata.
2. El usuario no deberá apuntar su contraseña en un papel, pósit, o en cualquier otro lugar no seguro.
3. El usuario no deberá escribir su contraseña en correos electrónicos ni en formularios web cuyo origen no sea confiable.
4. El usuario no deberá utilizar la misma contraseña para el acceso a distintos servicios o recursos.
5. El usuario no deberá utilizar la misma contraseña para el acceso a distintos dispositivos.
6. El usuario no deberá utilizar la misma contraseña para uso profesional y para uso personal o doméstico.
7. El usuario no deberá hacer uso de funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personas no autorizadas.
8. El usuario deberá proceder a cambiar la contraseña de forma inmediata si tiene indicios de que la confidencialidad de la misma ha podido verse comprometida.
9. Ningún usuario está autorizado a acceder al sistema de información utilizando el código o identificador de usuario y la contraseña de otros usuarios.

3. CAMBIO DE CONTRASEÑAS

A pesar de lo robusta que sea una contraseña, la confidencialidad de la misma puede verse comprometida con el paso del tiempo. En su consecuencia, las contraseñas deben ser cambiadas periódicamente. La periodicidad dependerá del tipo de datos a que den acceso:

- La contraseña deberá ser cambiada, con carácter general, como mínimo cada doce meses (un año).
- La contraseña deberá ser cambiada, como mínimo, cada seis meses, si se trata de una contraseña de acceso a «categorías especiales de datos personales» (ver art. 9 RGPD) o a datos muy personales, cuya violación implique graves repercusiones para el interesado (por ejemplo, datos bancarios).



4. ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Todos los usuarios del sistema de información del responsable del tratamiento deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente política de «Buenas prácticas en la gestión de contraseñas», debiendo suscribirla a través del siguiente modelo de «Aceptación y compromiso de cumplimiento».

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA POLÍTICA DE «BUENAS PRÁCTICAS EN LA GESTIÓN DE CONTRASEÑAS»

Mediante la cumplimentación de la presente declaración, el abajo firmante, como usuario del sistema de información de la entidad, dice haber leído y comprendido la Política de «Buenas prácticas en la gestión de contraseñas» de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

En _____, a ____ de _____ de 20__

Denominación de la entidad:	
NIF de la entidad:	
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario:	

Por la entidad:

D./ Dña. _____
DNI número: _____

5. CONTROLES REGULARES DE CUMPLIMIENTO

En virtud de lo establecido en el artículo 32, apartado 1, letra d), del Reglamento (UE) 2016/679, se recomienda la realización de controles regulares de cumplimiento en los puestos de trabajo, con el objetivo de verificar, evaluar y valorar la eficacia de la política de «Buenas prácticas en la gestión de contraseñas» para garantizar una seguridad y confidencialidad adecuadas de los datos personales objeto de tratamiento en la entidad y, en particular, para impedir el acceso o uso no autorizados de dichos datos.

A continuación, se expone un modelo de registro de los controles regulares de cumplimiento realizados sobre la gestión de contraseñas en la entidad responsable del tratamiento:

CONTROL REGULAR DE CUMPLIMIENTO GESTIÓN DE CONTRASEÑAS	
Fecha de realización (día/mes/año)	
Creación de contraseñas	
Resultado	Favorable ☐ Con salvedades ☐ Desfavorable ☐
Deficiencias	
Medidas correctoras o complementarias necesarias	
Uso de contraseñas	
Resultado	Favorable ☐ Con salvedades ☐ Desfavorable ☐
Deficiencias	
Medidas correctoras o complementarias necesarias	
Cambio de contraseñas	
Resultado	Favorable ☐ Con salvedades ☐ Desfavorable ☐
Deficiencias	
Medidas correctoras o complementarias necesarias	
Aceptación y compromiso de cumplimiento	
Resultado	Favorable ☐ Con salvedades ☐ Desfavorable ☐
Deficiencias	
Medidas correctoras o complementarias necesarias	

NORMATIVA APLICABLE

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD).