POLÍTICA DE CONTRASENYES DE LA UNIVERSITAT MIGUEL HERNÁNDEZ

Aprovada per acord de la Comissió de Seguretat de la UMH en la sessió de 17 de maig de 2022

1. OBJECTE I ÀMBIT D'APLICACIÓ

La present política pretén regular la creació i l'ús de contrasenyes robustes, quan aquest siga el mecanisme d'autenticació usat per a l'accés a determinats sistemes o serveis de la Universitat Miguel Hernández (UMH).

Aquesta política és aplicable a tot l'àmbit d'actuació de la Universitat Miguel Hernández, i els seus continguts es deriven directament de les directrius de caràcter més general definides en la Normativa general d'ús dels recursos i sistemes d'informació de la Universitat Miguel Hernández.

La present política és aplicable i de compliment obligat per a tot el personal que, de manera permanent o eventual, estiga vinculat amb la UMH, incloent-hi el personal d'organitzacions externes, quan siga usuari o posseïsca accés als sistemes d'informació de la UMH i utilitzen contrasenyes com a mitjà d'autenticació personal.

2. MARC NORMATIU

Són aplicables les lleis i normatives espanyoles, així com les que dimanen de la Unió Europea i de la Generalitat Valenciana en relació amb protecció de dades personals, propietat intel·lectual i ús d'eines telemàtiques, així com les que puguen

POLÍTICA DE CONTRASEÑAS DE LA UNIVERSIDAD MIGUEL HERNÁNDEZ

Aprobada por acuerdo de la Comisión de Seguridad de la UMH en su sesión de 17 de mayo de 2022

1. OBJETO Y ÁMBITO DE APLICACIÓN

La presente política pretende regular la creación y uso de contraseñas robustas, cuando este sea el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios de la Universidad Miguel Hernández (UMH).

Esta política será de aplicación a todo el ámbito de actuación de la Universidad Miguel Hernández, y sus contenidos se derivan directamente de las directrices de carácter más general definidas en la Normativa General de Uso de los Recursos y Sistemas de Información de la Universidad Miguel Hernández.

La presente política será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, esté vinculado con la UMH, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la UMH y utilicen contraseñas como medio de autenticación personal.

2. MARCO NORMATIVO

Son de aplicación las leyes y normativas españolas, así como las que dimanan de la Unión Europea y de la Generalitat Valenciana en relación con protección de datos personales, propiedad intelectual y uso de herramientas telemáticas, así como

aparéixer, en un futur, referents a això.

Aquesta normativa se situa dins del marc jurídic definit per les lleis i els reials decrets següents:

● Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat
● REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades)
● Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
• Acord d'aprovació del Consell de Govern de 27 d'octubre de 2021 de la modificació de la Política de seguretat de la informació de la Universitat Miguel Hernández.

● Acord d'aprovació del Consell de Govern de 23 de febrer de 2022 de la Normativa general d'ús dels recursos i sistemes d'informació de la Universitat Miguel Hernández.

3. ÚS DE CONTRASENYES

Una contrasenya és una forma d'autenticació dels usuaris, que utilitza informació secreta, per a controlar l'accés a serveis i aplicacions. La contrasenya s'ha de mantindre en secret i no ha de ser predictible a partir d'informació pública de l'usuari. Una contrasenya filtrada pot comprometre la seguretat de l'usuari i de tota la universitat.

las que puedan aparecer, en un futuro, a este respecto.

Esta normativa se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

● Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
● REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO 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)
● Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
• Acuerdo de aprobación del Consejo de Gobierno de 27 de octubre de 2021 de la modificación de la Política de Seguridad de la Información de la Universidad Miguel Hernández.
● Acuerdo de aprobación del Consejo de Gobierno de 23 de febrero de 2022 de la Normativa General de Uso de los Recursos y Sistemas de Información de la Universidad Miguel Hernández.

3. USO DE CONTRASEÑAS

Una contraseña es una forma de autenticación de los usuarios, que utiliza información secreta, para controlar el acceso a servicios y aplicaciones. La contraseña debe mantenerse en secreto y no debe ser predecible a partir de información pública del usuario. Una contraseña filtrada puede comprometer la seguridad del usuario y de toda la universidad.

Les contrasenyes juntament amb l'identificador d'usuari són el mitjà d'autenticació per al lloc de treball, l'accés a la xarxa corporativa, l'accés al compte de correu i, en general, els sistemes d'informació i serveis que s'ofereixen en la UMH.

Cap usuari està autoritzat a accedir als serveis interns de la UMH utilitzant usuari+contrasenya d'altres usuaris, incloent-hi el simple coneixement de la contrasenya d'un altre usuari. Aquesta pràctica compromet la confidencialitat de la informació i, per descomptat, l'autenticitat de qui hi accedeix.

Quan es demostre un ús incorrecte o no acceptable respecte al que especifica aquesta política, o quan es reba un avís d'incidència dels organismes encarregats d'això (CCN-CERT, RedIris), la UMH podrà bloquejar temporalment o indefinidament l'usuari depenent de la gravetat i reiteració de l'incident, del qual serà responsable l'usuari titular.

4. CREACIÓ DE CONTRASENYES ROBUSTES

Cal que les contrasenyes que s'utilitzen com a mecanisme d'autenticació siguen robustes, és a dir, difícilmente vulnerables.

Les contrasenyes han de complir obligatòriament els requisits següents:

1. La longitud de la contrasenya ha de ser com a mínim de 8 caràcters, si bé es recomana usar contrasenyes més llargues.
2. La contrasenya ha de contindre almenys 2 caràcters alfabètics els quals han de ser, com a mínim, una lletra majúscula i una minúscula.
3. La contrasenya ha de contindre almenys un caràcter numèric.

Las contraseñas junto con el identificador de usuario son el medio de autenticación, para el puesto de trabajo, el acceso a la red corporativa, el acceso a la cuenta de correo y, en general, los sistemas de información y servicios que se ofrecen en la UMH.

Ningún usuario está autorizado a acceder a los servicios internos de la UMH utilizando usuario+contraseña de otros usuarios, incluyendo el simple conocimiento de la contraseña de otro usuario. Esta práctica compromete la confidencialidad de la información, y por supuesto, la autenticidad de quién accede a ella.

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en esta política, o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-CERT, RedIris), la UMH podrá bloquear temporal o indefinidamente al usuario dependiendo de la gravedad y reiteración del incidente, siendo responsable el usuario titular.

4. CREACIÓN DE CONTRASEÑAS ROBUSTAS

Es necesario que las contraseñas que se utilicen como mecanismo de autenticación sean robustas, es decir, difícilmente vulnerables.

Las contraseñas deben cumplir obligatoriamente los siguientes requisitos:

1. La longitud de la contraseña debe ser como mínimo de 8 caracteres, si bien se recomienda usar contraseñas más largas.
2. La contraseña debe contener al menos 2 caracteres alfabéticos de los cuales serán, como mínimo, una letra mayúscula y una minúscula.
3. La contraseña debe contener al menos un carácter numérico.

4. La contrasenya ha de tindre almenys un caràcter especial (qualsevol altre caràcter que no siga alfabètic o numèric, per exemple: ! # $ % ^ & * ( ) _ + - = { } | [ ] \ : ; ? , . /
5. Caràcters no permesos: " ‘~@<>€ (espai en blanc)
6. La contrasenya s’ha de canviar almenys una vegada cada 12 mesos.
7. No es poden utilitzar les quatre últimes contrasenyes emprades.

5. RECOMANACIONS SOBRE L’ÚS DE CONTRASENYES

Es poden considerar les recomanacions següents per a l’elecció d’una contrasenya robusta:

• Com a norma general, les contrasenyes han de ser fàcils de recordar i d’introduir, encara que difícils d’endevinar i de descobrir per força bruta (prova exhaustiva de totes les possibilitats).

• Les contrasenyes no han d’estar compostes de dades pròpies que una altra persona puga endevinar o obtindre fàcilment (nom, cognoms, data de naixement, número de telèfon, DNI, etc.), ni ser frases famoses o refranys, ni ser estrofes de cançons o frases impactants de pel·lícules o d’obres de literatura.

• No s’han d’utilitzar per a generar la contrasenya paraules o noms comuns que puguen figurar en diccionaris.

• No s’ha de compartir la contrasenya de cap manera amb altres persones, encara que siguen del seu mateix entorn.

• Cal guardar la informació de contrasenyes en un lloc segur (mai en paper; es recomana l’ús de gestors de contrasenyes).

• És especialment important mantindre el caràcter secret de la contrasenya. No s’ha d’entregar ni comunicar a ningú. En cas d’haver tingut necessitat de fer-ho, l’usuari haurà de procedir a canviar-la de manera

4. La contraseña debe tener al menos un carácter especial (cualquier otro carácter que no sea alfabético o numérico, por ejemplo: ! # $ % ^ & * ( ) _ + - = { } | [ ] \ : ; ? , . /
5. Caracteres no permitidos:" '~@<>€ (espacio en blanco)
6. La contraseña deberá cambiarse al menos una vez cada 12 meses.
7. No se podrán utilizar las cuatro últimas contraseñas empleadas.

5. RECOMENDACIONES SOBRE EL USO DE CONTRASEÑAS

Pueden considerarse las siguientes recomendaciones para la elección de una contraseña robusta:

• Como norma general, las contraseñas deben ser fáciles de recordar y de introducir, aunque difíciles de adivinar y de descubrir por fuerza bruta (prueba exhaustiva de todas las posibilidades).

• Las contraseñas no deberán estar compuestas de datos propios que otra persona pueda adivinar u obtener fácilmente (nombre, apellidos, fecha de nacimiento, número de teléfono, DNI, etc.), ni ser frases famosas o refranes, ni ser estrofas de canciones o frases impactantes de películas o de obras de literatura.

• No utilizar para generar la contraseña palabras o nombres comunes que puedan figurar en diccionarios.

• No compartir la contraseña bajo ningún concepto con otras personas, aunque sean de su mismo entorno.

• Guardar la información de contraseñas en un lugar seguro (nunca en papel; se recomienda el uso de gestores de contraseñas).

• Es especialmente importante mantener el carácter secreto de la contraseña. No debe entregarse ni comunicarse a nadie. En caso de haber tenido necesidad de hacerlo, el usuario deberá proceder a cambiarla de

immediata.
• No s'ha d'utilitzar la mateixa contrasenya per a diferents serveis web o en l'accés a diferents dispositius.
• Les contrasenyes han de ser substituïdes per unes altres, bé pel mateix usuari o bé pels administradors dels sistemes de la UMH, si hi ha evidència que han sigut compromeses.

6. VIGÈNCIA

La present política entrarà en vigor l'endemà de la publicació en el *Butlletí Oficial de la Universitat Miguel Hernández* (BOUMH), amb l'aprovació prèvia per la Comissió de Seguretat de la UMH, i fins que siga reemplaçada per una nova política.

forma inmediata.
• No utilizar la misma contraseña para distintos servicios web o en el acceso a distintos dispositivos.
• Las contraseñas serán sustituidas por otras, bien por el mismo usuario o bien por los administradores de los sistemas de la UMH, si existe evidencia de que hubieran sido comprometidas.

6. VIGENCIA

La presente política entrará en vigor al día siguiente de su publicación en el *Boletín Oficial de la Universidad Miguel Hernández* (BOUMH), previa aprobación por la Comisión de Seguridad de la UMH, y hasta que sea reemplazada por una nueva política.

EL PRESIDENTE DE LA COMISIÓN DE SEGURIDAD DE LA UMH

Signat electrònicament per:/Firmado electrónicamente por:
Federico Botella Beviá