ARBONIA
IT SECURITY

Information Security Policy

Directiva de contraseñas

Versión:	1.0
publicada el:	08/07/2021
Status:	RELEASED
Clasificación:	RESTRICTED
Redactado por:	ICT Security Officer
Publicado por:	Arbonia IT Board
Directiva:	IS-ISP-GROUP-001-PASSWORD-POLICY
Revisión:	s/i

Información de directivas

Finalidad	La presente Directiva de contraseña explica y define fundamentos para la creación y el uso de contraseñas en el grupo Arbonia.
Usuarios/Destinatarios	▪ Todos los empleados del grupo Arbonia ▪ Contratistas externos/proveedores /clientes y socios que tengan acceso a los sistemas de ICT del grupo Arbonia
Archivo electrónico de documentos	https:\\security.arbonia.com

Registro de cambios

Versión	Fecha	Status	Modificación	realizada por
0.1	2021-06-14	Draft	Draft of the policy	ICT Security Officer
0.9	2021-07-07	Draft	Draft for adoption	ICT Security Officer
0.9	2021-07-07	Review		Arbonia IT Board
1.0	2021-07-08	Adoption		Arbonia IT Board

Índice

Glosario 4
1 Finalidad, campo de aplicación y usuarios 5
2 Fundamentos de gobierno 5
2.1 La importancia de las contraseñas 5
2.2 Obligaciones de los usuarios/titulares de cuentas 5
3 Directiva de contraseñas 6
3.1 Definición 6
3.2 Gestión de contraseñas 6
3.3 Especificaciones para contraseñas 7
3.4 Estrategia de contraseñas 8
3.5 Excepciones/Particularidades 8
4 Creación de contraseñas seguras 9
5 Documentos de referencia 9
6 Entrada en vigor 9
7 Anexos relevantes 10

Registro de abreviaturas

Término	Explicación
ICT	Informations and Communications Technology (Tecnología de información y comunicación)
OS	Operating System (Sistema operativo)
ISMS	Sistemas de gestión de seguridad de información

Glosario

Término	Explicación
Brute Force Attack	Un ataque con fuerza bruta consiste en un intento de hackear una contraseña o un nombre de usuario probando todas las combinaciones posibles.
Sistemas de gestión de seguridad de información	Un sistema de gestión de la seguridad de la información está formado por un compendio de procedimientos y reglas dentro de una organización que sirven para establecer, gestionar, controlar, mantener y mejorar continuamente y de forma duradera la seguridad de la información.

1 Finalidad, campo de aplicación y usuarios

La directiva describe los requisitos y especificaciones que deben cumplir las contraseñas de acceso a los sistemas de ICT del grupo Arbonia. También establece las reglas para garantizar una gestión, un uso y una creación de contraseñas seguras.

La presente directiva rige para todo el ámbito de aplicación de los sistemas de gestión de seguridad de información (ISMS), es decir, para todos los sistemas ICT del grupo Arbonia.

Los usuarios y destinatarios de esta directiva son todos los empleados del grupo Arbonia, así como los contratistas externos/proveedores/clientes/socios etc., que precisen acceso a los sistemas ICT del grupo Arbonia.

2 Fundamentos de gobierno

2.1 La importancia de las contraseñas

La seguridad de los sistemas ICT de Arbonia consiste fundamentalmente, entre otros factores, en un uso cuidadoso de las contraseñas, y en particular, en el respeto de los principios fundamentales para la utilización de contraseñas.

El objetivo prioritario de todo atacante es robar datos de acceso de un usuario para lograrse un acceso a los sistemas ICT del grupo Arbonia, y así localizar y aprovechar posibles puntos débiles. Intentan adueñarse de los permisos privilegiados de un administrador de sistemas, para en el peor de los casos poder realizar después de forma inadvertida actividades ilícitas como el robo de datos, espionaje o la instalación de software malicioso. Por ello, una contraseña débil o un uso indebido de esta, supone un riesgo considerable. Este riesgo se incrementa aún más con el uso de permisos privilegiados, que muchas veces son necesarios para realizar la actividad laboral.

Por todo ello resulta imprescindible evitar a toda costa el robo de datos de acceso y respetar las siguientes obligaciones.

2.2 Obligaciones de los usuarios/titulares de cuentas

Todos los usuarios están obligados a aplicar procedimientos seguros y probados a la hora de elegir y aplicar las contraseñas (véanse más detalles en el apartado 3):

- Hay que elegir siempre una contraseña "segura". La longitud y el formato de una contraseña se elegirá de forma que complique un ataque con fuerza bruta para que lleve mucho tiempo y resulte infructuoso
- Las contraseñas nunca se transmitirán a terceras personas. Tampoco deben comunicarse a superiores, a la dirección de la empresa o a los administradores de sistemas
- Las contraseñas no deben anotarse ni guardarse indebidamente (p. ej., en excel), a no ser que el dpto. informático haya autorizado para ello un método seguro (p. ej., una herramienta de contraseñas)
- Cada contraseña debe modificarse periódicamente
- También hay que cambiar una contraseña, si existieran indicios de que una contraseña hubiera sido hecha pública, es decir, si se ha transmitido a terceras personas
- Cualquier sospecha de uso indebido o abuso deben comunicarse inmediatamente al dpto. informático responsable
- En caso de que un usuario o una usuaria posea una cuenta de usuario dedicada con privilegios administrativos, no se deberá utilizar la misma contraseña que para la cuenta estándar
- El titular de la cuenta es siempre responsable de que se cumpla la presente Directiva de contraseñas, aunque esto no se exija a nivel técnico. En ningún caso se permite el uso de contraseñas estándar, vacías o débiles

3 Directiva de contraseñas

3.1 Definición

Se aplican distintas directivas de contraseñas en función de los privilegios precisados, a fin de conseguir un nivel de seguridad de la información adecuado. Se diferencia entre:

- uso general del tipo "usuario", sin privilegios administrativos para sistemas ICT
- aplicación específica del tipo "administrador", con privilegios administrativos para uno o más sistemas ICT. En relación con las cuentas de usuarios del tipo "administrador", se diferencia entre:
    - cuentas de proveedores/de sistemas/de servicios (usadas para funciones automáticas, instalación o administración de componentes en sistema ICT, como p. ej., OS, datos bancarios, aplicaciones o cuentas de redes, etc.)
    - las cuentas con derechos de administradores (usadas para personas individuales con el fin de permitirles permisos privilegiados en sus sistemas ICT)

3.2 Gestión de contraseñas

1. La contraseña está asignada a una cuenta ID única (usuario o administrador)
2. Tanto la ID de la cuenta como la contraseña son personales. Solo la persona responsable conocerá la contraseña.
3. La contraseña no se guardará escrita en texto legible
4. La validez de una contraseña nunca superará los 360 días, o bien 540 días (véase el apartado 3.3)
5. Se rechazará una contraseña nueva si ya se utilizó entre las cinco contraseñas anteriores
6. El número de intentos fallidos para generar una contraseña está limitado a seis intentos. Tras el sexto intento, se bloquea la cuenta hasta que la vuelva a desbloquear un administrador.
7. El contador de intentos de registro fallidos no debe restaurarse en menos de 60 minutos
8. Las contraseñas temporales pueden tener una validez de <72 h y el usuario debe ser instado, la primera vez que se registre, a cambiar la contraseña temporal. Esto será así siempre que técnicamente resulte aplicable. En caso contrario, cada titular de cuenta será responsable por sí mismo de este cambio de contraseña
9. Lo mismo regirá para la asignación automática de contraseñas para abrir una cuenta de usuario

Regulación especial para cuentas de proveedores/de sistemas/de servicios:

- Excepción a la regla n.º 2: las contraseñas ligadas a este tipo de cuentas, pueden almacenarse en una herramienta de contraseñas (encriptada) segura con acceso protegido por contraseña, y compartirse con varias personas a través de grupos de roles y permisos, siempre que esto resulte necesario para el desarrollo de su actividad
- Excepción a la regla n.º 4: las contraseñas ligadas a este tipo de cuentas, pueden tener activada la opción contraseñas sin caducidad, si es necesario
- Excepción a la regla n.º 6: las contraseñas ligadas a este tipo de cuentas, no tienen que bloquearse automáticamente

La aplicación de las excepciones se explica en el apartado 3.5.

3.3 Especificaciones para contraseñas

La contraseña para una cuenta del tipo "usuario" sin privilegios administrativos para sistemas ICT debe cumplir los requisitos siguientes:

- constar como mínimo de 12 caracteres con una validez de contraseña de 360 días, y/o como mínimo de 16 caracteres con una validez de 540 días
- tener una complejidad 4 de 4, lo que obliga a tener que utilizar los caracteres siguientes como mínimo una vez:
  - Mayúsculas
  - Minúsculas
  - Cifras de 0 a 9
  - signos de puntuación o caracteres especiales (no todos los sistemas ICT aceptan estos caracteres)
- no debe incluir el nombre de la cuenta
- no debe contener números en la primera y última posición
- ni tampoco 3 caracteres idénticos sucesivos

Las contraseñas para una cuenta del tipo "administrador" con privilegios administrativos para sistemas ICT están sujetas a las siguientes regulaciones adicionales:

Regulación especial para cuentas de proveedores/de sistemas/de servicios:

- constar al menos de 32 caracteres
- la contraseña se debe generar con un método aleatorio y documentar con una herramienta de contraseñas adecuada (véase la excepción a la regla n.º 2, apartado 3.2)

Regulación especial para cuentas de administrador:

- constar al menos de 15 caracteres

Regulación especial para sistemas terceros (B2C / B2B y otros) operados por el grupo Arbonia:

las especificaciones para contraseñas también son de aplicación fundamental para sistemas externos (terceros), pero pueden ser adaptadas a la situación circunstancial de cada Business Use Case, siempre que resulte necesario. En cualquier caso, las regulaciones especiales se tratarán tal y como especifica el apartado 3.5.

Especificaciones especiales para cuentas de Windows – implementadas interna y automáticamente en Arbonia:

- la nueva contraseña no debe figurar en una base de datos junto a contraseñas comprometidas. Esto lo evita la comprobación técnica a la hora de generar la contraseña
- la recién creada contraseña no debe aparecer en un diccionario definido por un usuario. Este diccionario se actualizada de manera centralizada y contiene, entre otros, el nombre de la empresa. En caso de coincidencia, se muestran directamente las palabras no permitidas
- la contraseña deberá modificarse, si ha aparecido en una base de datos junto a contraseñas comprometidas

3.4 Estrategia de contraseñas

Historial de contraseñas	5
Validez máxima de la contraseña	360 (12–15 caracteres), y/o 540 días (≥16 caracteres)
Validez mínima de la contraseña	0
Complejidad	4/4 (mayúsculas/minúsculas/cifras 0–9/signos de puntuación o caracteres especiales)
Longitud mínima de la contraseña o Usuario o Cuentas de proveedores/de sistemas/de servicio o Cuentas de administrador	 12 caracteres 32 caracteres (creada con método aleatorio) 15 caracteres
Cifrado inverso (Windows Domain)	desactivada
Cantidad de intentos de registro fallidos hasta que se bloquea la cuenta	6
Duración del bloqueo de la cuenta	Hasta que un administrador desbloquea
Tiempo que transcurre hasta que se restaura el contador con los intentos de registro fallidos	≥ 60 minutos
Particularidades (Windows Domain)	La contraseña no debe contener números en la primera y última posición La contraseña no debe incluir 3 caracteres idénticos sucesivos

3.5 Excepciones/Particularidades

Todos los procesos de autenticación asistidos por ordenador deberán cumplir, en la mayor medida posible, las directrices de la presente directiva, así como comprobar este cumplimiento. En caso de que no se dispongan de requisitos técnicos para la necesaria implementación, el titular de la cuenta deberá garantizar estas condiciones a través de un proceso manual y utilizar una contraseña segura dentro de las posibilidades de cada sistema.

El IT-Security Officer local podrá asignar autorizaciones excepcionales respecto de la presente directiva, siempre que se cumplan los fundamentos en cuanto a seguridad de la información y no exista riesgo para los sistemas ICT del grupo Arbonia. Este responsable decidirá, si lo considera necesario de común acuerdo con el responsable de seguridad del dpto. ICT, si se otorga una exención o bien, si se establecen otras medidas para minimizar el riesgo. Cualquier excepción deberá recogerse por escrito en un directorio.

4 Creación de contraseñas seguras

Existen diferentes técnicas para generar una contraseña segura y recordarla:

1.er ejemplo: Generar una contraseña segura basada en una oración o frase

Elija una frase que le resulte fácil de memorizar y transfórmela en su contraseña.

Por ejemplo: No es tan difícil elegir una contraseña realmente segura.

Utilice las letras iniciales o varias letras de cada palabra y complete la contraseña con números y caracteres especiales.

Por ejemplo, Netde1conrealS.

2.º ejemplo: Crear una contraseña segura sustituyendo caracteres

Elija una palabra que le resulte fácil de memorizar, por ejemplo, "automóvil" y defina una secuencia especial, p. ej. "1$1". Ahora sustituya determinadas partes o letras de la palabra con la secuencia especial que ha elegido para generar una contraseña segura.

Por ejemplo: aut1$1m1$1vil

Rogamos tenga presente que, para generar su contraseña, nunca debería utilizar información o datos a los que se pueden acceder libremente a través de los medios sociales. Encontrará más consejos en materia de seguridad de contraseñas en nuestros cursos formativos de IT Security Awareness.

5 Documentos de referencia

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Directiva para el uso de sistemas informáticos en el grupo Arbonia

6 Entrada en vigor

Nombre	División	Función	Fecha	Firma
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sanitary	CIO Division HVAC / Sanitary	2021-07-08	n/a
Tobias Shibli	Division Windows	CIO Division Windows	2021-07-08	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-07-08	n/a

7 Anexos relevantes

N.º	Explicación	Nombre del archivo
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	