

Nueva Directiva de contraseñas del grupo Arbonia

Estimados empleados:

de todos es sabido que una contraseña segura es la primera línea defensiva para nuestros sistemas y datos.

El objetivo prioritario de cualquier atacante es, entre otros, robar los datos de acceso a una cuenta de usuario a fin de garantizarse un acceso inicial a nuestras redes, servidores y sistemas informáticos para, en el peor de los casos efectuar, sin ser detectado, actividades delictivas como el robo de datos, espionaje o la instalación de software malicioso. Por ello, una contraseña débil o comprometida, así como un uso indebido de esta, supone un riesgo considerable. El grupo Arbonia ha establecido una nueva directiva de contraseñas precisamente para cumplir incluso mejor con nuestros requisitos de seguridad y protegernos aún mejor contra estas amenazas.

Modificación de la Directiva de contraseñas

Más adelante encontrará una representación sinóptica de nuestra estrategia de contraseñas íntegra. La modificación afecta principalmente a la longitud mínima de la contraseña, la validez máxima así como la complejidad de la misma.



La longitud mínima de la contraseña se ha incrementado de 8 a 12 caracteres para complicar el acceso a una contraseña, pero al mismo tiempo se prorroga la validez de cada contraseña como mínimo a 360 días. En caso de que utilice una contraseña más larga (≥ 16 caracteres), la vigencia de esta se prolonga a un total de 540 días. En todos los casos las nuevas contraseñas deben garantizar una alta complejidad (= contraseña segura). Esto se consigue combinando mayúsculas/minúsculas/cifras de 0 a 9/signos de puntuación o caracteres especiales.



Además, así se evita automáticamente el uso de contraseñas comprometidas previamente filtradas y de libre acceso en Internet, así como las palabras incluidas en una lista negra (p. ej. nombres de empresas).



En caso de que la contraseña durante su vigencia apareciera en una base de datos junto con contraseñas comprometidas, se le instará automáticamente a modificarla.

La nueva Directiva de contraseñas se activa automáticamente en cuanto cambie la próxima vez su contraseña de Windows, o bien mediante solicitud de su departamento informático local. En este sentido, recibirá un recordatorio 14 días antes de que caduque la contraseña. **Sin embargo, esta directiva rige para todos los sistemas ICT del grupo Arbonia, es decir, también para los sistemas que no sean de Windows.** En su calidad de titular de la cuenta, Usted es siempre responsable de que se cumpla la presente Directiva de contraseñas, aunque esto no se exija a nivel técnico.

Configurar una contraseña segura

Existen diferentes técnicas para generar una contraseña segura y recordarla. Por ejemplo, cree una contraseña segura basada en una frase o sustituyendo una secuencia de caracteres definida:

- Elija una frase que le resulte fácil de memorizar y transfórmela en su contraseña. Por ejemplo: *"No es tan difícil elegir una contraseña segura."* Utilice las letras iniciales o varias letras de cada palabra y complete la contraseña con números y caracteres especiales. Por ejemplo, *"Netde1conrealS."*
- Elija una palabra que le resulte fácil de memorizar, por ejemplo, "Primavera" y defina una secuencia especial, p. ej. *"1\$1"*. Ahora sustituya determinadas partes o letras de la palabra con la secuencia que ha elegido para generar una contraseña segura. Por ejemplo: *"aut1\$1m1\$1vil"*

Muchas gracias por tomar nota y saludos cordiales
Arbonia Security Team



Estrategia de contraseñas

Historial de contraseñas (cantidad de últimas contraseñas que no deben volver a utilizarse)	5	Cantidad de intentos de registro fallidos hasta que se bloquea la cuenta	6
Longitud mínima de la contraseña	12 caracteres	Duración del bloqueo de la cuenta	Hasta que un administrador desbloquea
Validez máxima de la contraseña	360 días (de 12 a 15 caracteres) y/o 540 días (≥16 caracteres)	Tiempo que transcurrir hasta que se restaura el contador con los intentos de registro fallidos	≥ 60 minutos
Complejidad	➤ Mayúsculas ➤ Minúsculas ➤ Cifras de 0 a 9 ➤ Signos de puntuación o caracteres especiales	Particularidades (contraseñas de Windows – Arbonia a escala interna y aplicación automática)	La contraseña no debe contener números en la primera y última posición, ni tampoco 3 caracteres idénticos sucesivos



No utilice las contraseñas indicadas a modo de ejemplo en el presente documento. Estas palabras a modo de ejemplo a partir de ahora son "comprometidas" y forman parte de la lista ne-



Además de este mensaje informativo, tenga en cuenta también la Directiva de contraseñas vigente (IS-ISP-GROUP-001-PASSWORD-POLICY) en <https://security.arbonia.com>



Cuando cambie su contraseña de Windows, se le mostrarán automáticamente los requisitos que deben cumplirse.

- ✓ Debe contener al menos 12 caracteres
- ✓ Debe contener al menos 1 mayúscula
- ✓ Debe contener al menos 1 minúscula
- ✓ Debe contener al menos 1 dígito
- ✓ Debe contener al menos 1 carácter especial
- ✓ No debe contener su nombre de usuario
- ✓ No debe contener 3 o más caracteres idénticos consecutivos
- ✓ No debe terminar con un dígito
- ✓ No debe comenzar con un dígito

Estas reglas se comprobarán una vez que envíe la contraseña

- No debe estar en la lista de contraseñas vulneradas

Una contraseña más larga durará más; esta contraseña caducará en **360** días.

360 540

✓ Las contraseñas coinciden

Powered by Specops Software



Change a password

CHAFG1\specops

Old password

.....

.....

Sign in to: CHAFG1

How do I sign in to another domain?

Cancel