1. Objetivo

El objetivo de esta política es establecer los lineamientos y procedimientos para la creación, uso, y gestión de contraseñas en **VIARIUM** y cuya finalidad es garantizar la seguridad e integridad de la información y los sistemas, protegiéndolos contra accesos no autorizados y posibles ciberataques.

2. Alcance

Esta política se aplica a todos los empleados, contratistas, consultores y cualquier otra persona con acceso a los sistemas, redes y datos de **VIARIUM**. Esto incluye, pero no se limita a, sistemas operativos, aplicaciones, bases de datos, plataformas de inteligencia artificial y cualquier otro recurso tecnológico de la entidad.

3. Responsabilidades

- **Usuarios**: Son responsables de crear y mantener contraseñas seguras, así mismo, de protegerlas y salvaguardarlas contra el acceso no autorizado y/o filtraciones.
- **Administradores de Sistemas**: Deben garantizar la implementación y el cumplimiento de esta política, proporcionando soporte y supervisión en la gestión de contraseñas.
- **Equipo de Seguridad Informática**: Monitorean y revisan el cumplimiento de la política, realizando auditorías periódicas y tomando medidas correctivas cuando sea necesario.

4. Políticas específicas de contraseñas

4.1. Requisitos de Creación de Contraseñas

- Las contraseñas deben tener al menos 12 caracteres.
- Deben incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales (por ejemplo, !, @, #, $) excepto los siguientes caracteres (; , ‟,”, |) reservados por algunos softwares específicos.
- No deben contener información personal identificable, como nombres, fechas de nacimiento, o números de identificación.
- No deben ser iguales a las 3 últimas contraseñas utilizadas previamente.
- Comunicada inicialmente mediante sistema de “one time password”.

4.2. Cambio y Caducidad de Contraseñas

- Las contraseñas deben cambiarse cada 90 días.
- Los usuarios no pueden reutilizar ninguna de sus últimas 3 contraseñas.
- En caso de sospecha de compromiso de una contraseña, debe cambiarse inmediatamente.

4.3. Almacenamiento y Protección de Contraseñas

- Las contraseñas no deben escribirse ni almacenarse en lugares accesibles fácilmente.
- Está prohibido compartir contraseñas a través de correos electrónicos o cualquier otro medio no seguro.

- Se recomienda el uso de gestores de contraseñas aprobados por el Equipo de Seguridad Informática para almacenar y gestionar contraseñas de manera segura.

4.4. Almacenamiento y Protección de Contraseñas

- Se debe implementar autenticación multifactor (MFA) en todos los sistemas críticos y de acceso remoto.
- El MFA debe combinar al menos dos de los siguientes factores: algo que el usuario sabe (contraseña), algo que el usuario tiene (token de seguridad, aplicación de autenticación), y algo que el usuario es (huella digital, reconocimiento facial).
- Solo se podrá hacer uso de MFA autorizados por el equipo de seguridad informática.

4.5. Acceso nominal a los sistemas

Una vez arrancado el equipo, el usuario deberá acceder a los recursos de trabajo del servidor mediante contraseña única personal. Combinación aleatoria de mayúsculas, minúsculas, números y caracteres especiales, que no se asemejen a palabras o nombres.

1. Única por usuario y cuenta, es decir, diferente entre aplicaciones.
2. Intransferible bajo ningún concepto.

4.6. Supervisión y Auditoría

- El Equipo de Seguridad Informática realizará auditorías periódicas para asegurar el cumplimiento de esta política.
- Los registros de acceso y uso de contraseñas deben mantenerse y revisarse regularmente para detectar y responder a cualquier actividad sospechosa.

4.7. Educación y Concienciación

- Todos los empleados deben recibir formación regular sobre la importancia de las contraseñas seguras y las prácticas recomendadas para su gestión.
- Se proporcionará material educativo y sesiones de capacitación para mantener la concienciación sobre la seguridad de contraseñas.

5. Manejo de Incidentes

5.1. Reporte de Incidentes:

- Cualquier sospecha de compromiso de una contraseña debe reportarse inmediatamente al Equipo de Seguridad Informática.
- Los usuarios deben cambiar su contraseña inmediatamente si creen que ha sido comprometida.

5.2. Respuesta a Incidentes:

- El Equipo de Seguridad Informática investigará todos los reportes de compromisos de contraseñas.

- Se tomarán medidas correctivas y preventivas para mitigar cualquier riesgo asociado con el compromiso de contraseñas.

6. Excepciones

Cualquier excepción a esta política debe ser aprobada por el Equipo de Seguridad Informática y debe estar documentada, indicando la razón de la excepción y las medidas compensatorias implementadas para asegurar la protección de la información.

7. Revisión y actualización

Esta política será revisada y si es necesario, actualizada cuando proceda o cuando se produzcan cambios significativos en el entorno tecnológico o se materialicen alguna amenaza de seguridad. Con esta política, **VIARIUM** se compromete a garantizar la seguridad de sus sistemas y la información que maneja, implementando prácticas robustas de gestión de contraseñas para protegerse contra accesos no autorizados y ciberataques.

La Dirección, a 12 de febrero de 2025.