SEGURIDAD INFORMATICA Y PLAN ESTRATÉGICO DE TI

Ing. Giomar Aldair Luis Gavino

Ing. Franklin Pérez Rojas

Ing. Jeiner Huancas Montenegro

MINISTERIO DE SALUD

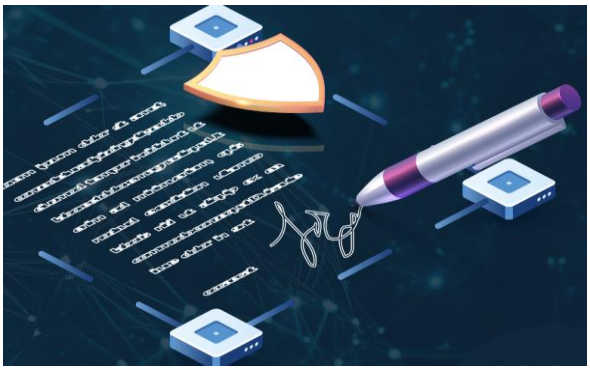
DIRECCIÓN DE REDES INTEGRADAS DE SALUD

LIMA CENTRO

POLITICA:

POLÍTICA DE CONTRASEÑAS

AÑO: 2025



DIRECCIÓN ADMINISTRATIVA

OFICINA DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Elaborado por la Oficina de Gestión de Tecnologías de la Información	Revisado por la Oficina de Planeamiento y Modernización de la Gestión Pública	Aprobado por la Dirección General	Acto Resolutivo que lo Aprueba	Fecha de Aprobación
			Resolución Directoral N° _____ – 2025-DG-DIRIS-LC	

Campo	Detalle
Código	PO07
Versión	1.0
Fecha de emisión	15/12/2025
Vigencia	Indefinida
Estado	Activo
Oficina responsable	OGTI

1. INTRODUCCIÓN

La Dirección de Redes Integradas de Salud Lima Centro (DIRIS Lima Centro) administra hospitales, establecimientos de primer nivel y centros especializados, coordinando a más de , profesionales. La Oficina de Gestión de Tecnologías de la Información (OGTI) es responsable de la seguridad digital para garantizar la confidencialidad, integridad y disponibilidad de la información institucional. Frente a la creciente amenaza de ciberataques, es fundamental establecer normas claras para la gestión de contraseñas, protegiendo así los datos de miles de ciudadanos.

1.1. Autoridad

La Dirección de Redes Integradas de Salud (DIRIS) Lima Centro, como órgano desconcentrado del Ministerio de Salud del Perú, tiene la responsabilidad de garantizar la seguridad de la información y la protección de datos sensibles relacionados con los servicios de salud, gestión administrativa y atención ciudadana.

En el marco de la Ley de Protección de Datos Personales (Ley N.° 29733) y la ISO/IEC 27001:2022, la DIRIS Lima Centro establece la presente política de contraseñas como parte de su Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con los controles de acceso (A.5 y A.8).

1.2. Propósito

El propósito de esta política es definir los lineamientos y requisitos para la creación, uso, protección y gestión de contraseñas en los sistemas de información de la DIRIS Lima Centro, con el fin de:

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Reducir el riesgo de accesos no autorizados a sistemas y datos sensibles.
- Cumplir con las mejores prácticas internacionales de ciberseguridad e ISO/IEC 27001.

1.3. Alcance

Esta política aplica a:

- Todo el personal de la DIRIS Lima Centro, incluyendo trabajadores de planta, contratados, practicantes y terceros autorizados.
- Todos los sistemas, aplicaciones, dispositivos y servicios que almacenen, procesen o transmitan información institucional.
- Los accesos a servicios en la nube, sistemas clínicos, administrativos, financieros y de soporte.

2. Políticas de contraseñas

Política 1. Longitud mínima y frases de contraseña

Las contraseñas deberán tener una longitud mínima de 12 caracteres, de preferencia en forma de frase de contraseña. Una mayor longitud incrementa exponencialmente el tiempo necesario para un ataque de fuerza bruta.
Según NIST, las frases largas son más seguras y fáciles de recordar que combinaciones cortas. Esto fortalece la confidencialidad (ISO 27001 – A.8.2.2).

Política 2. Complejidad obligatoria

Las contraseñas deberán incluir mayúsculas, minúsculas, números y caracteres especiales para evitar combinaciones predecibles.
La diversidad de caracteres eleva la entropía de la contraseña, dificultando ataques de diccionario.

Política 3. Prohibición de información personal

Está prohibido usar datos personales en contraseñas, como nombres, fechas de nacimiento o DNI.
Esta práctica reduce la exposición a ataques de ingeniería social y phishing, que suelen basarse en datos públicos.

Política 4. Evitar palabras comunes

No se permite el uso de contraseñas con palabras de diccionario o patrones simples (“123456”, “qwerty”).

El 80% de los ataques exitosos utilizan combinaciones predecibles. El bloqueo de estas claves fortalece el control de acceso.

Política 5. Creatividad y variaciones

Se recomienda el uso de errores ortográficos intencionales, fonética alterada o símbolos alternativos.

Genera contraseñas memorables para el usuario pero difíciles de adivinar por un atacante.

Política 6. Confidencialidad estricta

Las contraseñas son personales e intransferibles. Está prohibido compartirlas o enviarlas por correo, WhatsApp o notas escritas. Minimiza el riesgo de fuga interna, uno de los principales vectores de incidentes en instituciones públicas.

Política 7. Contraseña única por sistema

Cada sistema o aplicación crítica deberá tener una contraseña distinta. el “efecto dominó”: si una contraseña es comprometida, no se pone en riesgo toda la red de sistemas.

Política 8. Autenticación multifactor (MFA)

Todos los accesos a información crítica deberán reforzarse con MFA. Incluso si la contraseña es robada, el atacante no podrá acceder sin el segundo factor. Este control es recomendado por ISO 27001 en A.5.17.

Política 9. Uso de gestores de contraseñas

Los usuarios deberán almacenar sus contraseñas únicamente en el gestor institucional aprobado.

Evita la reutilización de claves y mejora la administración de contraseñas largas y complejas.

Política 10. Historial de contraseñas

No se podrá reutilizar ninguna de las últimas cinco contraseñas. Previene el retroceso a contraseñas antiguas que podrían estar comprometidas en filtraciones previas.

Política 11. Periodicidad de cambio

Las contraseñas deberán renovarse cada 180 días o antes si hay incidentes.

Limita la ventana de exposición si una contraseña ha sido comprometida sin detección inmediata.

Política 12. Bloqueo por intentos fallidos

Las cuentas se bloquearán tras cinco intentos fallidos consecutivos. Disuade ataques automatizados de fuerza bruta y obliga a reportar accesos no autorizados.

Política 13. Contraseñas de cuentas privilegiadas

Las cuentas administrativas deberán cambiar sus contraseñas cada 90 días.

Cuentas con permisos elevados son objetivos de alto riesgo; su rotación frecuente mitiga ataques internos y externos.

Política 14. Desactivación de cuentas inactivas

Cuentas inactivas por más de 60 días serán bloqueadas automáticamente.

Reduce la superficie de ataque cerrando accesos huérfanos que podrían ser explotados.

Política 15. Verificación contra contraseñas comprometidas

Antes de ser aceptada, cada contraseña será verificada contra listas de contraseñas filtradas.

Evita que los usuarios creen contraseñas que ya circulan en la dark web o bases de datos comprometidas.

Política 16. Prohibición de almacenamiento inseguro

Está prohibido almacenar contraseñas en papel, notas visibles o archivos sin cifrar.

Protege contra accesos físicos y fugas por descuido en oficinas y dispositivos.

Política 17. Contraseñas temporales seguras

Las contraseñas generadas por TI para accesos provisionales deberán ser complejas, únicas y forzar el cambio en el primer uso. Evita que contraseñas estándar ("admin123") sean un punto débil recurrente.

Política 18. Doble control para accesos críticos

Los accesos a sistemas estratégicos deberán autorizarse bajo un esquema de doble validación (usuario + supervisor).

Aumenta la trazabilidad y dificulta accesos indebidos en sistemas de misión crítica.

Política 19. Auditoría periódica

Se realizarán revisiones semestrales para validar la correcta aplicación de esta política.

Asegura la mejora continua en el marco del ciclo PDCA de la ISO 27001.

Política 20. Concientización y capacitación

Todo el personal deberá capacitarse en buenas prácticas de contraseñas al menos dos veces al año.

La capacitación reduce el factor humano como vulnerabilidad, que es responsable de más del 70% de los incidentes de ciberseguridad.

3. Cumplimiento

- El cumplimiento será evaluado mediante **auditorías internas**, **revisiones de accesos** y **monitoreo continuo**.
- Se aplicará el **principio de mejora continua** (PDCA) del SGSI conforme a la ISO 27001.
- Las sanciones seguirán el **Reglamento Interno de Trabajo** y, en casos graves, se derivarán a la **Oficina de Recursos Humanos** y la **Oficina de Control Interno**.

Nº	Política	Prioridad	Sanción en caso de incumplimiento	Excepciones
1	Longitud mínima de 12 caracteres	Alta	Advertencia formal y cambio inmediato de contraseña	No
2	Complejidad obligatoria (mayúsculas, minúsculas, números, símbolos)	Alta	Bloqueo temporal de cuenta hasta corrección	No
3	Prohibición de información personal	Alta	Solicitud inmediata de cambio y notificación a TI	No
4	Evitar palabras comunes o patrones	Alta	Bloqueo automático y restablecimiento de credenciales	No
5	Uso creativo (errores ortográficos, fonética)	Media	Recomendación de cambio en capacitación	Sí (si cumple reglas de entropía)
6	Confidencialidad estricta (no compartir)	Alta	Medida disciplinaria; posible suspensión	No
7	Contraseña única por sistema	Alta	Capacitación obligatoria y cambio forzado	No
8	Autenticación multifactor (MFA)	Alta	Denegación de acceso a sistemas críticos	No

9	Uso de gestor de contraseñas institucional	Media	Reentrenamiento obligatorio	Sí (con autorización de TI por sistemas no integrados)
10	Historial: no reutilizar últimas 5	Alta	Solicitud de cambio inmediato	No
11	Cambio obligatorio cada 180 días	Media	Bloqueo automático de cuenta hasta actualización	Sí (para cuentas de servicio, con aprobación de TI)
12	Bloqueo tras 5 intentos fallidos	Alta	Bloqueo temporal de cuenta + reporte	No
13	Cuentas privilegiadas: cambio cada 90 días	Alta	Suspensión de privilegios de administrador	No
14	Desactivación de cuentas inactivas > 60 días	Media	Desactivación automática	Sí (si se justifica y aprueba por Recursos Humanos y TI)
15	Verificación contra contraseñas comprometidas	Alta	Denegación de nueva contraseña hasta corrección	No
16	Prohibición de almacenamiento inseguro (papel, notas, etc.)	Alta	Procedimiento disciplinario interno	No
17	Contraseñas temporales seguras (forzar	Alta	Bloqueo inmediato de la cuenta	No

	cambio en primer uso)			
18	Doble control en accesos críticos	Alta	Denegación de acceso sin segunda validación	Sí (solo en casos de contingencia con autorización escrita)
19	Auditoría periódica de cumplimiento	Media	Informe a jefe de área y plan correctivo	No
20	Capacitación obligatoria 2 veces/año	Media	Registro negativo en evaluación de desempeño	Sí (en caso de licencias médicas o excepciones justificadas)