

Política de seguridad de la información

Lineamientos de uso responsable, controles de cuenta, consecuencias y marco normativo de referencia.

Versión	Ámbito	Uso
2.1.1	Portal de Salud	Usuarios autorizados

Contenido

- 1. 1. Finalidad y alcance
- 2. 2. Obligaciones del usuario
- 3. 3. Conductas no permitidas
- 4. 4. Consecuencias operativas dentro del portal
- 5. 5. Marco normativo peruano de referencia
- 6. 6. Ejemplos de riesgo y efectos
- 7. 7. Gestión de incidentes
- 8. 8. Buenas prácticas mínimas

1. Finalidad y alcance

Esta política orienta a los usuarios autorizados sobre el uso seguro y responsable del Portal de Salud. No sustituye las normas internas de la entidad ni determina por sí sola responsabilidades administrativas, civiles o penales.

La calificación de una conducta concreta depende de los hechos, el vínculo del usuario con la entidad y la autoridad competente.

2. Obligaciones del usuario

- Usar la cuenta únicamente para las funciones autorizadas.
- Mantener la contraseña en reserva.
- Cambiar la contraseña temporal en el primer ingreso.
- Verificar la información antes de registrarla.
- No consultar ni difundir datos sin autorización.
- Cerrar sesión en equipos compartidos.
- Reportar accesos o actividad sospechosa.

3. Conductas no permitidas

- Compartir o prestar credenciales.
- Intentar acceder a cuentas, datos o funciones ajenas.
- Alterar, suprimir o introducir información falsa de forma deliberada.
- Copiar, extraer o divulgar datos personales fuera de la finalidad autorizada.
- Evitar controles de acceso, auditoría o seguridad.
- Usar el sistema para una finalidad personal, comercial o distinta de la labor autorizada.

4. Consecuencias operativas dentro del portal

Situación	Medida posible
Contraseña temporal pendiente	Acceso limitado hasta cambiarla.
Actividad sospechosa	Revisión de auditoría y sesiones.
Incumplimiento de seguridad	Suspensión o bloqueo de la cuenta.
Pérdida de credenciales	Restablecimiento con contraseña temporal.
Acceso no autorizado	Bloqueo, preservación de registros y escalamiento a la instancia competente.

Estas medidas técnicas no reemplazan las decisiones administrativas o legales que pueda adoptar la entidad competente.

5. Marco normativo peruano de referencia

Ley N.º 29733 - Ley de Protección de Datos Personales

Establece obligaciones para el tratamiento de datos personales. El acceso, uso o divulgación de información personal debe responder a una finalidad legítima y a las condiciones aplicables al tratamiento.

Decreto Supremo N.º 016-2024-JUS

Aprueba el Reglamento de la Ley N.º 29733 y desarrolla obligaciones vinculadas al tratamiento y seguridad de datos personales.

Ley N.º 30096 - Ley de Delitos Informáticos y modificatorias

Sanciona diversas conductas ilícitas que afectan sistemas y datos informáticos. Dependiendo de los hechos, un acceso deliberadamente no autorizado, la alteración de datos u otras conductas pueden tener relevancia penal.

Decreto Legislativo N.º 1412 - Ley de Gobierno Digital y su reglamento

Establece el marco de gobierno digital para entidades públicas, incluyendo gestión de identidad digital, servicios digitales, seguridad digital y datos.

Ley N.º 27815 - Código de Ética de la Función Pública

Cuando resulte aplicable al usuario, establece principios, deberes y prohibiciones para servidores públicos, incluyendo responsabilidad, discreción y uso adecuado de bienes e información vinculados al ejercicio del cargo.

6. Ejemplos de riesgo y efectos

Conducta	Riesgo / efecto
Compartir contraseña	Pérdida de trazabilidad y uso de la cuenta por terceros.
Consultar datos sin necesidad funcional	Posible acceso indebido y afectación de la privacidad.
Modificar información deliberadamente	Afectación de la integridad documental y de la auditoría.
Extraer datos para uso externo	Riesgo de tratamiento o divulgación no autorizada.
Ocultar un incidente	Aumenta el impacto y dificulta la contención.

7. Gestión de incidentes

- Cierra las sesiones si observas actividad que no reconoces.
- Cambia la contraseña cuando todavía tengas acceso.
- Comunica el incidente a soporte o al responsable designado.
- No borres evidencias ni alteres registros de auditoría.

- Sigue las instrucciones de la entidad para la investigación y contención.

8. Buenas prácticas mínimas

- Usa una contraseña única.
- No almacenes credenciales en archivos compartidos.
- Evita iniciar sesión desde equipos desconocidos.
- Revisa la identidad y la información antes de registrar un documento.
- Mantén la sesión cerrada cuando no estés trabajando.
- Consulta solo la información necesaria para tu función.

Normativa de referencia revisada para esta versión: Ley N.º 29733, D.S. N.º 016-2024-JUS, Ley N.º 30096 y modificatorias, D. Leg. N.º 1412 y Ley N.º 27815. La aplicación concreta debe evaluarse según cada caso.