POLÍTICA DE SEGURIDAD Y GESTIÓN DE LA INFORMACIÓN

DXMédica

Dato	Información
Documento	Política de Seguridad y Gestión de la Información
Organización	DXMédica
Versión	0.9
Estado	Aprobado
Autoridad de aprobación	Dr. Pablo Lespi
Responsable operativo	Ladislao Potocki
Referentes para incidentes	Dr. Pablo Lespi y Ladislao Potocki
Fecha de elaboración	14 de Marzo de 2026
Revision	3 de Junio 2026
Revisión	Anual o ante cambios significativos

---

1. Objeto

La presente política tiene por objeto establecer los principios, responsabilidades y medidas generales destinadas a proteger la información gestionada por el Laboratorio DXMédica.

Las medidas de seguridad estarán orientadas a preservar:

- La **confidencialidad**, evitando que la información sea conocida por personas no autorizadas.
- La **integridad**, evitando alteraciones, pérdidas o modificaciones indebidas.
- La **disponibilidad**, procurando que la información y los sistemas estén accesibles cuando sean necesarios.
- La **trazabilidad**, permitiendo identificar las acciones realizadas sobre la información.
- La **autenticidad**, procurando verificar la identidad de quienes generan, modifican, validan o consultan información.

La seguridad de la información será considerada una responsabilidad institucional y no exclusivamente tecnológica.

2. Alcance

Esta política alcanza a:

- Todo el personal de DXMédica.
- Médicos patólogos.
- Técnicos y profesionales.
- Personal administrativo.
- Personal del Equipo de Tecnología de la Información.
- Autoridades y responsables de área.
- Proveedores, contratistas y profesionales externos.
- Estudiantes, pasantes o investigadores que accedan a información del laboratorio.
- Pacientes y profesionales que utilicen los portales habilitados.
- Sistemas, aplicaciones, servidores, redes y dispositivos.
- Bases de datos, copias de seguridad y registros de auditoría.
- Documentación clínica, técnica y administrativa.
- Muestras, vidrios, casetes, tacos, etiquetas y demás elementos asociados a protocolos.
- Información en formato digital, papel, imágenes, fotografías o cualquier otro soporte.

La política será aplicable tanto a los recursos ubicados dentro de la sede como a los servicios externos utilizados para almacenamiento, respaldo, comunicación o procesamiento.

---

3. Marco normativo y de referencia

El tratamiento de información deberá realizarse respetando la normativa nacional, provincial, sanitaria y profesional aplicable.

Como marco general se considerarán:

- Ley 25.326 de Protección de los Datos Personales y su reglamentación.
- Ley 26.529 de Derechos del Paciente, Historia Clínica y Consentimiento Informado y sus modificaciones.
- Normas, disposiciones y recomendaciones de la Agencia de Acceso a la Información Pública.
- Normativa sanitaria y profesional aplicable a los laboratorios de anatomía patológica.

- Obligaciones contractuales asumidas con pacientes, instituciones, profesionales y proveedores.
- Principios y buenas prácticas de ISO/IEC 27001 e ISO/IEC 27002, sin que ello implique que el laboratorio se encuentre certificado.

Los datos vinculados con la salud son datos personales sensibles y requieren medidas especiales de protección. Toda persona que intervenga en la elaboración, manipulación, custodia o acceso a documentación clínica deberá mantener su confidencialidad.

El laboratorio deberá verificar y mantener actualizado, cuando corresponda, el registro de sus bases de datos personales ante la autoridad competente.

---

4. Principios generales

DXMédica aplicará los siguientes principios:

4.1. Necesidad y minimización

Solo se recopilarán y tratarán los datos necesarios para cumplir las finalidades asistenciales, diagnósticas, administrativas, científicas, legales o contractuales correspondientes.

4.2. Acceso restringido

La información será accesible únicamente para quienes la necesiten para cumplir sus funciones.

4.3. Mínimo privilegio

Los usuarios tendrán únicamente los permisos indispensables para realizar sus tareas.

4.4. Responsabilidad individual

Cada usuario será responsable de las acciones realizadas con su cuenta y de proteger sus credenciales.

4.5. Seguridad desde el diseño

Los nuevos sistemas, desarrollos e integraciones deberán incorporar controles de seguridad desde las etapas iniciales de análisis y desarrollo.

4.6. Trazabilidad

Las operaciones relevantes deberán quedar registradas para permitir auditorías, investigaciones y reconstrucción de eventos.

4.7. Continuidad

La información crítica deberá contar con mecanismos de respaldo y recuperación.

4.8. Mejora continua

Las medidas de seguridad serán revisadas periódicamente y actualizadas ante cambios tecnológicos, normativos, operativos o institucionales.

---

5. Autoridades y responsabilidades

5.1. Autoridad institucional

El Dr. Pablo Lespi será la autoridad responsable de aprobar la presente política y respaldar institucionalmente su cumplimiento.

Será informado de los incidentes relevantes, riesgos significativos y decisiones que puedan afectar la seguridad, continuidad o confidencialidad de la información.

5.2. Equipo de Tecnología de la Información

El Equipo de Tecnología de la Información dirigido por Ladislao Potocki será responsable de:

- Administrar la infraestructura tecnológica.
- Mantener servidores, contenedores, redes y aplicaciones.
- Gestionar accesos administrativos.
- Ejecutar altas, modificaciones y bajas de usuarios.
- Mantener las reglas de firewall.
- Gestionar las copias de seguridad.
- Ejecutar pruebas de restauración.
- Coordinar actualizaciones tecnológicas.
- Mantener registros técnicos y de auditoría.
- Participar en la gestión de incidentes.
- Aplicar medidas correctivas.
- Informar riesgos relevantes a la autoridad.

5.3. Responsables de área

Los jefes o responsables de cada área deberán:

- Solicitar las altas y modificaciones de usuarios.
- Definir los permisos requeridos por cada persona.
- Informar cambios de funciones.

- Informar licencias prolongadas cuando corresponda restringir accesos.
- Comunicar las desvinculaciones o bajas de personal.

El responsable del área donde se produzca una desvinculación deberá comunicarla al Equipo de Tecnología de la Información, preferentemente antes de que se haga efectiva.

Cuando no sea posible informar anticipadamente, la comunicación deberá realizarse de forma inmediata y simultánea con la desvinculación.

5.4. Usuarios

Todos los usuarios deberán:

- Utilizar únicamente su cuenta personal.
- Proteger sus credenciales.
- No compartir contraseñas.
- Acceder solamente a la información necesaria para sus tareas.
- Bloquear la sesión al retirarse del equipo.
- Comunicar incidentes, errores o accesos sospechosos.
- Utilizar únicamente los sistemas y canales autorizados.
- Respetar la confidencialidad de la información incluso después de finalizada su relación con el laboratorio.

---

6. Clasificación de la información

La información será clasificada, como mínimo, en las siguientes categorías:

6.1. Información pública

Información cuya divulgación no representa un riesgo significativo.

Ejemplos:

- Dirección del laboratorio.
- Horarios de atención.
- Información institucional pública.
- Cartera general de servicios.

6.2. Información de uso interno

Información destinada al funcionamiento interno y que no debe divulgarse sin autorización.

Ejemplos:

- Procedimientos internos.
- Organigramas.
- Instructivos.
- Información operativa.

6.3. Información confidencial

Información cuyo acceso o divulgación indebida podría afectar al laboratorio, a sus empleados o a terceros.

Ejemplos:

- Información laboral.
- Contratos.
- Información económica.
- Configuraciones técnicas.
- Credenciales y documentación de sistemas.

6.4. Información sensible o altamente confidencial

Información que requiere el mayor nivel de protección.

Ejemplos:

- Datos identificatorios de pacientes.
- Información de salud.
- Diagnósticos.
- Informes anatomopatológicos.
- Imágenes clínicas.
- Datos genéticos o moleculares.
- Antecedentes médicos.
- Datos de autenticación.
- Correspondencia entre códigos de protocolo e identidad del paciente.

---

7. Protección de datos personales

Los datos personales serán utilizados exclusivamente para las finalidades que justificaron su recopilación.

El laboratorio deberá procurar que los datos sean:

- Exactos.
- Completos.

- Pertinentes.
- Actualizados cuando corresponda.
- No excesivos para la finalidad prevista.
- Conservados durante los plazos aplicables.
- Eliminados o anonimizados cuando hayan dejado de ser necesarios y no exista obligación de conservarlos.

Los pacientes podrán ejercer sus derechos de acceso, rectificación, actualización o supresión en los casos y condiciones previstos por la normativa aplicable.

No procederá la eliminación cuando exista una obligación legal, sanitaria, contractual o médico-asistencial de conservar la información.

---

8. Seudonimización e identificación de protocolos

Siempre que la finalidad lo permita, se evitará exponer directamente los datos identificatorios del paciente.

Para la identificación y trazabilidad de estudios se utilizará un código único asociado al protocolo.

Este código podrá utilizarse en:

- Códigos QR.
- Etiquetas.
- Vidrios.
- Casetes.
- Tacos.
- Imágenes.
- Registros técnicos.
- Contenedores de muestras.
- Documentación interna.
- Procesos de integración entre sistemas.

La correspondencia entre el código del protocolo y la identidad del paciente deberá mantenerse protegida y solamente podrá ser consultada por usuarios autorizados.

El uso de un código de protocolo constituye una medida de **seudonimización** y no una anonimización completa, debido a que existe la posibilidad de volver a relacionarlo con la identidad del paciente.

Por ese motivo, la información seudonimizada continuará siendo tratada como información sensible.

9. Gestión de usuarios

Todos los usuarios deberán disponer de una cuenta personal e individual.

Queda prohibido el uso habitual de cuentas compartidas o genéricas para acceder a información clínica, administrativa o técnica.

9.1. Alta de usuarios

Las altas deberán ser solicitadas mediante un mensaje interno dirigido al área de Tecnología de la Información.

La solicitud deberá permitir identificar:

- Persona para la que se solicita el acceso.
- Área a la que pertenece.
- Función o rol.
- Sistemas a los que necesita acceder.
- Permisos requeridos.
- Responsable que autoriza la solicitud.
- Fecha de inicio, cuando corresponda.

9.2. Modificación de permisos

Los cambios de función o responsabilidad deberán comunicarse al Equipo de Tecnología de la Información para adecuar los permisos.

Los accesos que hayan dejado de ser necesarios deberán retirarse.

9.3. Baja de usuarios

Ante una desvinculación, el jefe del área será responsable de informar la baja.

El Equipo de Tecnología de la Información deberá:

- Desactivar las cuentas.
- Revocar sesiones abiertas.
- Revocar accesos administrativos.
- Retirar o invalidar credenciales.
- Recuperar, cuando corresponda, equipos y dispositivos institucionales.
- Verificar que no permanezcan accesos mediante aplicaciones, VPN, API o servicios externos.

Las cuentas no deberán eliminarse cuando sea necesario conservar su identificación en registros históricos o de auditoría. En esos casos deberán mantenerse deshabilitadas.

9.4. Revisión de permisos

Los permisos deberán revisarse periódicamente y siempre que se produzcan cambios relevantes de funciones, sistemas o estructura organizativa.

---

10. Contraseñas y autenticación

Las contraseñas serán personales, confidenciales e intransferibles.

Los usuarios deberán:

- Utilizar contraseñas que no sean fáciles de adivinar.
- Evitar reutilizar contraseñas institucionales en servicios personales.
- Cambiar la contraseña inicial.
- Cambiarla ante cualquier sospecha de compromiso.
- No anotarla en lugares visibles.
- No comunicarla por teléfono, correo, WhatsApp o mensajería.
- No permitir que otra persona utilice su sesión.

El portal de pacientes recomendará a los usuarios mantener actualizada su contraseña y utilizar una contraseña diferente de la empleada en otros servicios.

Los sistemas deberán aplicar medidas para limitar intentos reiterados de acceso y disponer de procedimientos seguros de recuperación de cuentas.

La implementación de doble factor de autenticación se encuentra en estudio dentro del desarrollo del nuevo sistema centralizado de inicio de sesión.

El sistema centralizado deberá evaluar, al menos:

- Autenticación de doble factor.
- Administración centralizada de usuarios.
- Bloqueo de cuentas.
- Revocación central de sesiones.
- Registro de accesos.
- Políticas diferenciadas según el nivel de privilegio.
- Integración segura entre aplicaciones.

---

11. Infraestructura tecnológica

El laboratorio dispone de un servidor dedicado en el que se ejecutan aplicaciones y servicios mediante contenedores aislados.

Entre los servicios alojados se encuentran:

- Bases de datos.
- Aplicaciones web.
- Sistema de pacientes.
- Sistema de gestión del laboratorio.
- Sistema de trazabilidad y carga desde quirófano.
- Integraciones con sistemas externos.
- API de NAVIFY.
- Otros servicios necesarios para la operación.

La separación en contenedores tendrá como finalidad:

- Segregar aplicaciones.
- Limitar el impacto de fallas.
- Reducir accesos innecesarios entre servicios.
- Facilitar el mantenimiento.
- Aplicar permisos y reglas de red específicas.
- Mejorar la continuidad y recuperación de servicios.

El aislamiento mediante contenedores será una medida complementaria y no reemplazará la actualización, el firewall, la autenticación, los registros, las copias de seguridad y demás controles.

---

12. Acceso administrativo

El acceso administrativo a los servidores estará limitado al personal autorizado del Equipo de Tecnología de la Información.

El acceso remoto se realizará mediante SSH utilizando:

- Un puerto no estándar.
- Restricciones de firewall.
- Direcciones IP previamente autorizadas.
- Credenciales individuales.
- Medidas de autenticación acordes con el nivel de privilegio.

El uso de un puerto no estándar será considerado una medida complementaria y no una protección suficiente por sí sola.

Las bases de datos, paneles de administración y servicios internos no deberán exponerse públicamente salvo que exista una necesidad justificada y se implementen controles específicos.

Los permisos administrativos deberán otorgarse aplicando el principio de mínimo privilegio.

---

13. Seguridad de redes y dispositivos

Las computadoras pertenecientes al laboratorio deberán conectarse preferentemente mediante redes cableadas.

La conexión por cable tendrá como objetivos mejorar:

- La estabilidad.
- La disponibilidad.
- El control de acceso.
- La segmentación.
- La identificación de equipos.

Los equipos personales de empleados, profesionales, pacientes, proveedores o visitantes deberán conectarse exclusivamente a una red aislada.

La red para equipos personales no deberá permitir acceso directo a:

- Servidores.
- Bases de datos.
- Sistemas clínicos.
- Sistemas de trazabilidad.
- Sistemas administrativos internos.
- Equipos de procesamiento.
- Copias de seguridad.
- Interfaces administrativas.

No estará permitido conectar equipos personales directamente a la red interna sin autorización del Equipo de Tecnología de la Información.

---

14. Copias de seguridad

El laboratorio mantendrá copias de seguridad de la información y de los sistemas críticos.

El esquema incluirá:

- Copias completas semanales de bases de datos y archivos.
- Copias incrementales diarias.
- Copias horarias de los registros binarios de las bases de datos.

Los registros binarios permitirán complementar las copias completas e incrementales y recuperar operaciones hasta puntos determinados dentro del período disponible. Este mecanismo se conoce como recuperación a un punto en el tiempo o **Point-in-Time Recovery —PITR—**.

14.1. Almacenamiento

Las copias se almacenarán en un servidor externo a la infraestructura principal.

Los archivos de respaldo deberán conservarse cifrados.

El acceso estará restringido al personal autorizado.

Las credenciales y claves necesarias para recuperar las copias deberán protegerse y conservarse separadamente de los datos respaldados, cuando sea técnicamente posible.

14.2. Retención

Se conservarán:

- Las últimas cuatro copias completas.
- Las copias incrementales necesarias para completar los ciclos de recuperación asociados a las copias completas conservadas.
- Los registros binarios correspondientes al período definido para la recuperación de las bases de datos.

Las copias incrementales o registros binarios no deberán eliminarse mientras sean necesarios para restaurar una copia completa que continúe dentro del período de retención.

14.3. Pruebas de restauración

Se realizará como mínimo una prueba de restauración cada seis meses.

La prueba deberá verificar:

- Disponibilidad de las copias.
- Integridad de los archivos.
- Posibilidad de descifrado.
- Restauración de bases de datos.
- Restauración de archivos.
- Aplicación de incrementales.
- Recuperación mediante registros binarios, cuando corresponda.
- Documentación del procedimiento.
- Tiempo necesario para recuperar el servicio.

Cada prueba deberá generar un registro con:

- Fecha.
- Sistemas evaluados.
- Copias utilizadas.
- Personas intervinientes.
- Resultado.
- Problemas encontrados.
- Acciones correctivas.
- Fecha prevista para corregir las observaciones.

---

15. Registro de actividad y auditoría

Los sistemas deberán mantener registros de las acciones relevantes.

Cuando resulte técnicamente posible, los registros deberán identificar:

- Usuario.
- Fecha y hora.
- Sistema o módulo.
- Acción realizada.
- Registro afectado.
- Valor anterior.
- Valor nuevo.
- Equipo o dirección de origen.
- Resultado de la operación.

Deberán registrarse especialmente:

- Inicios de sesión.
- Intentos fallidos.
- Altas, bajas y modificaciones de usuarios.
- Cambios sobre datos clínicos.
- Modificaciones de informes.
- Validaciones.
- Cambios de diagnóstico.
- Descargas o entregas de informes.
- Acciones administrativas.
- Fallas de sistemas.
- Operaciones de restauración.

Los registros deberán protegerse contra alteraciones y accesos no autorizados.

Su consulta estará limitada a fines de:

- Auditoría.
- Seguridad.
- Calidad.
- Investigación de incidentes.
- Resolución de errores.
- Cumplimiento normativo.
- Continuidad operativa.

---

16. Actualizaciones y mantenimiento

Las actualizaciones de servidores, aplicaciones, bases de datos y componentes de infraestructura serán coordinadas entre Ladislao Potocki y el Dr. Pablo Lespi.

Siempre que sea posible, las actualizaciones se realizarán en días y horarios no laborables para reducir el impacto sobre la operación.

Antes de una actualización relevante deberá evaluarse:

- Impacto esperado.
- Sistemas afectados.
- Dependencias.
- Disponibilidad de backups.
- Posibilidad de reversión.
- Tiempo estimado de interrupción.
- Necesidad de informar al personal.
- Validaciones posteriores.

Las vulnerabilidades críticas o incidentes activos podrán justificar actualizaciones urgentes fuera del esquema habitual.

Toda intervención significativa deberá quedar documentada.

---

17. Gestión de cambios

Los cambios relevantes en sistemas o infraestructura deberán ser planificados y autorizados.

Esto incluye:

- Instalación de nuevas aplicaciones.

- Cambios de red.
- Modificaciones de firewall.
- Actualizaciones de bases de datos.
- Nuevas integraciones.
- Cambios en APIs.
- Migraciones de servidores.
- Cambios de autenticación.
- Modificaciones de procesos de backup.
- Cambios que afecten la trazabilidad.

Cuando corresponda, deberán realizarse pruebas en un entorno separado antes de aplicar cambios en producción.

---

18. Comunicación con pacientes

Las comunicaciones con pacientes mediante WhatsApp, correo electrónico o teléfono deberán realizarse exclusivamente utilizando canales institucionales del Laboratorio DXMédica.

No deberán utilizarse números telefónicos, cuentas de correo o perfiles personales para comunicaciones habituales con pacientes.

WhatsApp podrá utilizarse para:

- Coordinación administrativa.
- Información sobre horarios.
- Confirmación de recepción de muestras.
- Aviso de disponibilidad de resultados.
- Indicaciones generales.
- Gestión de turnos.
- Consultas que no requieran revelar información clínica sensible.

No deberán enviarse por WhatsApp:

- Informes anatomopatológicos.
- Diagnósticos.
- Imágenes clínicas.
- Resultados médicos.
- Documentación sensible.
- Credenciales o contraseñas.
- Información clínica detallada.

Los informes deberán ser consultados mediante el portal de pacientes, previa autenticación.

Antes de brindar información relacionada con un estudio deberá aplicarse una verificación razonable de identidad.

---

19. Portal de pacientes

El portal será el medio habilitado para la consulta y descarga de informes.

El portal deberá:

- Exigir autenticación.
- Utilizar comunicaciones cifradas.
- Identificar al usuario.
- Limitar intentos fallidos.
- Registrar accesos relevantes.
- Aplicar recuperación segura de contraseña.
- Evitar exponer datos en direcciones, mensajes de error o registros públicos.
- Cerrar o invalidar sesiones cuando corresponda.
- Aplicar permisos según la relación del usuario con el informe.

La implementación del nuevo sistema centralizado de inicio de sesión deberá mejorar la administración de identidades y evaluar la incorporación de doble factor.

---

20. Digitalización y reducción del papel

El laboratorio promoverá la sustitución progresiva de registros en papel por sistemas digitales que permitan identificar y trazar muestras, preparados, vidrios, casetes, tacos y demás elementos mediante códigos QR u otros identificadores únicos.

La digitalización tendrá como objetivos:

- Mejorar la trazabilidad.
- Reducir errores de identificación.
- Evitar exposición innecesaria de datos personales.
- Mejorar la disponibilidad de la información.
- Mantener registros de auditoría.
- Facilitar búsquedas.
- Reducir la circulación de papel.
- Mejorar la recuperación ante incidentes.

La eliminación de documentación en papel deberá realizarse únicamente cuando el registro digital sea completo, íntegro, accesible, respaldado y válido conforme a los plazos legales y operativos aplicables.

Antes de eliminar documentación deberá verificarse:

- Legibilidad.
- Integridad.
- Asociación correcta con el protocolo.
- Existencia de copias de seguridad.
- Cumplimiento de los plazos de conservación.
- Autorización del responsable.
- Posibilidad de recuperar el documento.
- Ausencia de impedimentos legales, sanitarios o contractuales.

La documentación con datos personales deberá destruirse mediante un procedimiento que impida su reconstrucción o consulta.

---

21. Conservación de tacos y vidrios

Los tacos y vidrios correspondientes a biopsias y citologías, con excepción de los estudios PAP, se conservarán durante un período mínimo de diez años.

Cumplido el período mínimo, el área de Patólogos será responsable de decidir si:

- Se extiende su conservación.
- Se seleccionan determinados elementos para conservación permanente.
- Se autoriza su destrucción.

El área de Patólogos deberá indicar el procedimiento adecuado de conservación o destrucción.

La decisión deberá considerar:

- Utilidad diagnóstica.
- Posibles interconsultas.
- Necesidades médico-legales.
- Requisitos de calidad.
- Valor científico o docente.
- Normativa vigente.
- Condiciones físicas del material.

La destrucción deberá quedar registrada e identificar, como mínimo:

- Protocolos o períodos alcanzados.
- Fecha.
- Responsable que autorizó.
- Método utilizado.
- Personal interviniente.

Los estudios PAP se regirán por el plazo y procedimiento específico que establezca el laboratorio conforme a la normativa y los criterios profesionales aplicables.

---

22. Integraciones y terceros

Toda integración con terceros, incluida la API de NAVIFY, deberá ser evaluada antes de su implementación.

La evaluación deberá considerar:

- Datos transmitidos.
- Finalidad.
- Necesidad de incluir datos identificatorios.
- Posibilidad de seudonimización.
- Método de autenticación.
- Cifrado de comunicaciones.
- Custodia de claves.
- Registro de operaciones.
- Ubicación donde se procesan o almacenan los datos.
- Condiciones contractuales.
- Procedimiento ante incidentes.
- Eliminación o devolución de datos al finalizar el servicio.

Las credenciales de API no deberán incorporarse directamente en código fuente público ni compartirse por canales no autorizados.

Los terceros con acceso a información deberán asumir obligaciones de confidencialidad y seguridad acordes con la sensibilidad de los datos.

---

23. Gestión de incidentes

Se considerará incidente de seguridad cualquier evento que afecte o pueda afectar la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información.

Ejemplos:

- Acceso no autorizado.
- Pérdida de credenciales.
- Malware o ransomware.
- Eliminación accidental.
- Alteración de informes.
- Envío de información al destinatario equivocado.
- Pérdida de equipos.
- Caída de servidores.
- Falla de backups.
- Exposición de datos.
- Error de identificación de muestras.
- Pérdida de trazabilidad.
- Acceso indebido de un empleado o proveedor.
- Exposición de una clave de API.
- Pérdida de un taco, vidrio o muestra.
- Uso de cuentas compartidas.
- Ingreso no autorizado a la red interna.

23.1. Comunicación

Todo incidente deberá ser comunicado de forma inmediata al:

- Dr. Pablo Lespi.
- Ladislao Potocki.

La comunicación deberá efectuarse mediante los canales institucionales disponibles.

Los empleados no deberán ocultar incidentes ni intentar resolverlos sin informar cuando puedan existir consecuencias sobre pacientes, diagnósticos, muestras, sistemas o datos personales.

23.2. Actuación inicial

Ante un incidente se deberá:

1. Registrar la fecha y hora.
2. Identificar los sistemas o procesos afectados.
3. Contener el incidente cuando sea posible.
4. Evitar destruir registros o evidencias.
5. Preservar logs, archivos y equipos.
6. Determinar si existen datos personales afectados.
7. Evaluar el impacto sobre pacientes y operación.
8. Recuperar los servicios de forma controlada.

9. Documentar las decisiones adoptadas.
10. Definir acciones correctivas.

Las comunicaciones externas deberán ser autorizadas por la autoridad del laboratorio.

Cuando corresponda por normativa, contrato o decisión institucional, se evaluará la comunicación a pacientes, instituciones, proveedores o autoridades competentes.

---

24. Continuidad operativa

El laboratorio deberá contar con mecanismos que permitan continuar o recuperar sus procesos críticos ante una interrupción.

Deberán contemplarse, como mínimo:

- Caída del servidor principal.
- Interrupción de Internet.
- Falla eléctrica.
- Pérdida de bases de datos.
- Indisponibilidad del portal.
- Falla del sistema de trazabilidad.
- Indisponibilidad de servicios externos.
- Ataque informático.
- Daños físicos.
- Imposibilidad de acceso a la sede.

Cuando se utilicen procedimientos manuales durante una interrupción, la información deberá incorporarse posteriormente a los sistemas, manteniendo su identificación y trazabilidad.

---

25. Confidencialidad

Toda persona que acceda a información del laboratorio deberá mantener reserva sobre ella.

La obligación comprende:

- Datos de pacientes.
- Diagnósticos.
- Imágenes.
- Protocolos.

- Información laboral.
- Información comercial.
- Configuraciones técnicas.
- Credenciales.
- Incidentes.
- Información de proveedores.
- Documentación interna.

La obligación continuará vigente después de finalizar la relación laboral, contractual, profesional o académica.

No deberán realizarse fotografías, copias o capturas de información clínica salvo que exista una finalidad autorizada.

---

26. Capacitación y concientización

El personal deberá recibir información o capacitación sobre:

- Confidencialidad.
- Protección de datos personales.
- Uso de contraseñas.
- Identificación de intentos de fraude.
- Uso de correo y WhatsApp.
- Gestión segura de muestras.
- Uso de códigos QR.
- Notificación de incidentes.
- Manejo de información en papel.
- Uso de dispositivos personales.
- Responsabilidades de los usuarios.

Las capacitaciones podrán adaptarse según las funciones y riesgos de cada área.

---

27. Incumplimientos

El incumplimiento de esta política podrá dar lugar a:

- Restricción o suspensión de accesos.
- Revisión de permisos.
- Capacitación adicional.
- Medidas administrativas.

- Acciones disciplinarias.
- Acciones contractuales.
- Comunicación a autoridades, cuando corresponda.

Las medidas deberán aplicarse respetando las normas laborales, contractuales y legales vigentes.

---

28. Excepciones

Toda excepción deberá:

- Tener una justificación.
- Identificar el riesgo.
- Contar con autorización.
- Establecer medidas compensatorias.
- Tener una duración definida.
- Ser revisada periódicamente.

Las excepciones no podrán utilizarse para evitar controles sin una causa operativa o técnica válida.

---

29. Documentos y procedimientos asociados

La presente política deberá complementarse progresivamente con:

1. Procedimiento de altas, modificaciones y bajas de usuarios.
2. Procedimiento de gestión de contraseñas.
3. Procedimiento de copias de seguridad.
4. Procedimiento de restauración.
5. Procedimiento de gestión de incidentes.
6. Procedimiento de actualizaciones y cambios.
7. Procedimiento de entrega de informes.
8. Procedimiento de uso de WhatsApp, correo y teléfono.
9. Procedimiento de conservación y destrucción de tacos y vidrios.
10. Procedimiento de digitalización y destrucción de papel.
11. Procedimiento de gestión de proveedores e integraciones.
12. Inventario de activos y sistemas.
13. Matriz de usuarios, roles y permisos.
14. Plan de continuidad operativa.

---

30. Revisión

La política será revisada como mínimo una vez al año.

También deberá revisarse cuando ocurra:

- Un incidente de seguridad relevante.
- Una modificación normativa.
- Un cambio significativo de infraestructura.
- La incorporación de un nuevo sistema.
- La incorporación de doble factor.
- Una nueva integración externa.
- Un cambio en los procesos del laboratorio.
- Una modificación en las autoridades o responsables.
- Una observación de auditoría.

Toda nueva versión deberá ser aprobada por la autoridad correspondiente y comunicada al personal.
