POLÍTICA DE SEGURIDAD DIGITAL

CONTROL DE CAMBIOS DE DOCUMENTOS

VERSION	ORIGEN DE LOS CAMBIOS	FECHA DE REGISTRO			CARGO DEL FUNCIONARIO
		DIA	MES	AÑO	
01	Creación del documento	04	11	2025	Sistemas

1. OBJETIVO

La presente **Política de Seguridad Digital** tiene como finalidad establecer los lineamientos, principios, responsabilidades y controles que permitan proteger la información clínica, administrativa y tecnológica del **Hospital Departamental San Rafael**, garantizando la **confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia** de los sistemas y activos digitales frente a amenazas internas o externas.

Asimismo, busca asegurar el cumplimiento de la normativa legal vigente en materia de protección de datos personales, historia clínica, ciberseguridad y gestión pública.

2. ALCANCE

Esta política aplica a:

- Todo el personal del hospital: empleados, contratistas, estudiantes, pasantes, proveedores y terceros con acceso a los sistemas o información del Hospital Departamental San Rafael.
- Todos los recursos tecnológicos, incluyendo redes, servidores, sistemas clínicos, aplicaciones, bases de datos, dispositivos médicos conectados, equipos de cómputo y dispositivos móviles institucionales.
- Toda la información generada, procesada o almacenada en el marco de la atención médica, gestión administrativa y prestación de servicios hospitalarios.

3. PRINCIPIOS DE SEGURIDAD

A. **Confidencialidad:** La información de pacientes, personal y operaciones del hospital solo será accesible a personas autorizadas.
B. **Integridad:** Los datos clínicos y administrativos deben ser exactos, completos y estar protegidos contra modificaciones no autorizadas.
C. **Disponibilidad:** Los sistemas de información y servicios digitales del hospital deberán estar disponibles para su uso cuando sean necesarios para la atención en salud.
D. **Autenticidad:** Toda transacción, registro o comunicación digital debe ser verificable y atribuible a un usuario autorizado.
E. **Trazabilidad:** Las actividades relevantes en los sistemas deben quedar registradas y ser auditables.
F. **Cumplimiento legal:** Se respetarán las normas aplicables en materia de protección de datos personales, historia clínica, ciberseguridad, transparencia y contratación pública.

4. ROLES Y RESPONSABILIDADES

Rol	Responsabilidades principales
Gerencia / Dirección General	Aprobar esta política y garantizar los recursos humanos, técnicos y financieros necesarios para su implementación.
Responsable de Seguridad Digital / CISO Hospitalario	Coordinar, supervisar y evaluar el cumplimiento de esta política y los planes de ciberseguridad.
Área de Tecnologías de la Información (TI)	Implementar y administrar los sistemas tecnológicos, aplicar controles de seguridad, realizar respaldos y asegurar la continuidad operativa.
Comité de Seguridad de la Información	Evaluar riesgos, aprobar planes de acción y coordinar la respuesta a incidentes.
Usuarios (personal médico, administrativo y técnico)	Cumplir las normas establecidas, proteger sus credenciales, hacer uso adecuado de los recursos digitales y reportar incidentes o anomalías.
Proveedores y contratistas	Cumplir con las cláusulas y requisitos de seguridad definidos en los contratos o convenios con el hospital.

5. GESTIÓN DE RIESGOS

- Se realizará una **evaluación periódica de riesgos digitales y clínicos** para identificar amenazas, vulnerabilidades y su impacto potencial en la atención médica y la operación institucional.
- Se implementarán medidas preventivas, detectivas y correctivas para mitigar los riesgos identificados.
- Los incidentes de seguridad digital se gestionarán conforme al **Procedimiento de Gestión de Incidentes de Seguridad del Hospital**, garantizando la notificación oportuna a las autoridades competentes cuando corresponda.

6. CONTROL DE ACCESO

- El acceso a los sistemas de información hospitalarios se basará en el **principio de mínimo privilegio** y la **necesidad de conocer**.
- Todos los usuarios deberán contar con **credenciales únicas e intransferibles**, protegidas mediante contraseñas seguras y, cuando sea posible, **autenticación multifactor (MFA)**.

- Las cuentas de usuarios inactivos, exempleados o personal en rotación deberán ser deshabilitadas de forma inmediata.
- El acceso remoto solo estará permitido mediante canales seguros y autorizados.

7. PROTECCIÓN DE DATOS PERSONALES Y DE HISTORIA CLÍNICA

- El hospital garantizará el cumplimiento de la **Ley de Protección de Datos Personales** y de la normativa sobre **manejo y custodia de historias clínicas**.
- Los datos de salud son considerados **información sensible** y serán tratados exclusivamente para fines asistenciales, científicos o administrativos legítimos.
- Se implementarán medidas técnicas y organizativas para prevenir el acceso no autorizado, pérdida o alteración de los datos personales de pacientes y empleados.

8. USO ACEPTABLE DE LOS RECURSOS DIGITALES

- Los equipos, redes y sistemas informáticos del hospital se usarán únicamente para actividades institucionales autorizadas.
- Está prohibido instalar software no licenciado o ajeno a las actividades del hospital.
- Todo correo electrónico institucional y dispositivo conectado a la red hospitalaria deberá cumplir con las políticas de seguridad, antivirus y actualizaciones vigentes.
- No se permitirá el uso de medios de almacenamiento externos sin autorización expresa del área de TI.

9. GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL

- Todo incidente (pérdida de información, acceso indebido, malware, alteración de registros clínicos, etc.) debe ser **reportado de inmediato** al responsable de Seguridad Digital.
- Se documentarán los eventos, se analizarán sus causas y se aplicarán medidas correctivas y preventivas.
- En casos que involucren datos personales o historias clínicas, se procederá conforme a los protocolos de notificación a las autoridades de control y protección de datos.

10. CAPACITACIÓN Y CONCIENCIACIÓN

- El hospital promoverá una **cultura institucional de seguridad digital**, fomentando la responsabilidad y buenas prácticas entre todo el personal.
- Se impartirán **capacitaciones periódicas** en temas de ciberseguridad, manejo seguro de la información, phishing, protección de datos personales y uso responsable de la tecnología.

11. REVISIÓN, AUDITORÍA Y ACTUALIZACIÓN

- Esta política será revisada **anualmente** o cuando se presenten cambios significativos en la infraestructura tecnológica, la normativa legal o los procesos hospitalarios.
- El cumplimiento de la política será verificado mediante **auditorías internas y externas** de seguridad digital y protección de datos.

Elaboró: *Sandra Milena Rincón - Sistemas*
Reviso: *Jesús Viafara Ruiz – Asesor de calidad*
Aprobó: *Comité de gestión y desempeño*