PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD DE SALUD DE IBAGUE 2025

“NUESTROS SERVICIOS AL ALCANCE DE TODOS”
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: sistemas@usiese.gov.co

INTRODUCCIÓN

La Unidad de Salud de Ibagué (USI) reconoce que la seguridad y la privacidad de la información son fundamentales para ofrecer servicios médicos eficaces, proteger los datos personales de los pacientes y garantizar la disponibilidad de la infraestructura tecnológica crítica. Este plan se propone ofrecer un marco de seguridad robusto que integre las mejores prácticas en cuanto a tecnología, normativas de protección de datos, y un enfoque preventivo frente a amenazas emergentes en la infraestructura de Tics.

2. OBJETIVOS DEL PLAN

El objetivo principal del Plan de Seguridad y Privacidad de la Información es proteger los datos confidenciales, garantizar la integridad de los sistemas de información y asegurar la disponibilidad ininterrumpida de la infraestructura de tecnología de la información. Los objetivos específicos incluyen:

- **Garantizar la confidencialidad, integridad y disponibilidad** de la información médica de los pacientes y empleados.
- Asegurar el cumplimiento de la ley **2272 de 2017** (y otras normas nacionales/internacionales).
- Establecer **procedimientos y controles** de seguridad eficaces para minimizar riesgos de vulnerabilidad, especialmente en servicios sensibles como los sistemas **Dinámica Gerencial** y **Orfeo**.
- **Mejorar la educación y sensibilización** del personal en cuanto al uso de tecnologías, privacidad y protección de datos.

3. ALCANCE DEL PLAN

Este plan cubre todos los aspectos relacionados con el manejo y protección de la información dentro de la infraestructura TIC de la Unidad de Salud de Ibagué, incluyendo:

- **Infraestructura tecnológica**, incluidas redes, servidores físicos y virtualizados, sistemas de comunicaciones (radioenlaces), y almacenamiento de datos.
- **Sistemas de información**, incluyendo Dinámica Gerencial para gestión de citas y salud, Orfeo para gestión documental, y los sistemas asociados a la página web de citas y base de datos de pacientes.
- **Políticas de acceso y control de usuarios** para todo el personal médico, administrativo, y asistencial.

4. EVALUACIÓN DE RIESGOS

Se llevará a cabo una **evaluación detallada de riesgos** en base a las siguientes categorías:

- **Riesgos internos**: Acceso no autorizado o abuso de privilegios por parte del personal.
- **Riesgos externos**: Ciberataques, como ransomware, phishing, o acceso ilegal por parte de terceros.
- **Riesgos operacionales**: Fallos de infraestructura tecnológica (por ejemplo, caídas de servidor) o desastres naturales que puedan afectar la infraestructura crítica.

Cada riesgo será evaluado según su **probabilidad de ocurrir** y **el impacto** sobre la organización. Por ejemplo:

- **Riesgo Alto**: Pérdida de información médica clave por vulnerabilidades de red.
- **Riesgo Medio**: Acceso no autorizado a documentos confidenciales sin consecuencias inmediatas graves.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Políticas clave:

- **Contraseñas seguras y autenticación multifactor (MFA)**: Todas las contraseñas deben ser robustas (mínimo 8 caracteres con letras, números y símbolos), con un cambio regular y autenticación adicional en servicios sensibles.
- **Control de accesos**: Utilización de políticas basadas en el principio de **mínimos privilegios** (sólo acceso necesario para realizar el trabajo), con monitoreo regular de los registros de acceso.
- **Cifrado de datos**: Toda la información médica, datos personales y comunicaciones confidenciales debe ser cifrada tanto en reposo (almacenada) como en tránsito (al ser enviada por correo o a través de redes).

- **Gestión de respaldos (Backups)**: Implementación de copias de seguridad diarias tanto en servidores locales como en un datacenter alterno (ubicado en una zona fuera de la red principal) para asegurar la continuidad ante posibles desastres.
- **Seguridad de redes y dispositivos**: Uso de **firewalls**, **VPNs**, **antivirus actualizados** y sistemas de detección de intrusos (IDS) para asegurar las comunicaciones de la red y proteger los dispositivos móviles o de escritorio del personal.

6. ESTRATEGIA DE GESTIÓN DE PRIVACIDAD

- **Cumplimiento de la legislación**: Implementación de medidas adecuadas para cumplir con la **Ley 1581 de 2012** sobre protección de datos personales y las normativas internacionales como el **GDPR** (si fuera aplicable).
- **Consentimiento informado**: Todos los pacientes deberán proporcionar su consentimiento para el tratamiento de datos personales, especialmente aquellos relacionados con su historial clínico.
    - Ejemplo: En el registro en línea para agendar citas, se solicitará consentimiento explícito para el tratamiento de datos.
- **Derechos de los pacientes**: Los pacientes deben poder acceder, modificar o eliminar sus datos a través de un proceso sencillo y seguro (por ejemplo, acceso al portal de atención para modificación de datos o solicitudes de eliminación de registros antiguos).
- **Minimización de la recopilación de datos**: No se recopilarán datos fuera de los estrictamente necesarios para ofrecer el servicio de salud requerido, y todos los datos personales serán gestionados de acuerdo con las finalidades específicas para las cuales fueron recolectados.

7. PLAN DE ACCIÓN

- **Implementación inicial**: Comenzar con la instalación de controles técnicos como firewalls y antivirus, además de capacitar al personal en buenas prácticas de seguridad.
- **Entrenamiento y concientización**: Cada miembro del personal recibirá capacitación continua en seguridad de la información, control de accesos y privacidad de datos. Se organizarán seminarios trimestrales y campañas de concientización.
- **Pruebas y auditorías de seguridad**: Realización de auditorías periódicas de seguridad cada seis meses para verificar que los controles sean efectivos.

8. RESPUESTA A INCIDENTES

- **Protocolo de manejo de incidentes**: En caso de detectar un incidente de seguridad (p.ej., ataque de malware o acceso no autorizado), se procederá de la siguiente manera:
    1. Aislar el sistema afectado para evitar la propagación.
    2. Notificar a los responsables técnicos e iniciar la investigación.
    3. Documentar todos los incidentes para analizar las causas y prevenir futuros problemas.
- **Notificación a las autoridades**: Según sea necesario, se procederá a informar a las entidades reguladoras o autoridades competentes en caso de filtración o violación de datos personales.

9. CUMPLIMIENTO NORMATIVO Y LEGAL

Este plan se alineará con las **normas nacionales** (como la Ley 1581 de 2012) y otros marcos internacionales aplicables a la protección de datos y a la seguridad de la información. Se seguirán los estándares internacionales de seguridad como la **ISO/IEC 27001** y las políticas de gestión del riesgo de información.

10. MONITOREO Y MEJORA CONTINUA

Este plan se revisará y actualizará de manera continua para asegurarse de que siga siendo adecuado y eficaz frente a las amenazas cambiantes. Las actualizaciones regulares del software, así como el seguimiento continuo de las amenazas externas, son parte de las actividades programadas en el ciclo de vida del plan.

CONCLUSIÓN

El **Plan de Seguridad y Privacidad de la Información** es fundamental para garantizar que la información médica, datos personales de los pacientes y la infraestructura tecnológica se mantengan seguras. La implementación adecuada de políticas, procedimientos y medidas de control permitirá fortalecer la protección frente a las amenazas y asegurar el cumplimiento con las normativas vigentes.

SAUL BETANCOURTH CARO
Profesional Universitario Sistemas