POLÍTICAS Y PROCEDIMIENTOS ACTUALIZADOS

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

1. Introducción

Este documento establece las políticas y procedimientos de seguridad de la información para la Unidad de Salud de Ibagué (USI). Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos, así como la protección de la infraestructura tecnológica frente a amenazas internas y externas. Estas políticas se alinean con las normativas y regulaciones aplicables en Colombia, incluyendo la Ley 1581 de 2012 de Protección de Datos Personales y las mejores prácticas internacionales como la norma ISO/IEC 27001.

2. Objetivos

1. Asegurar la protección de la información sensible y crítica de la Unidad de Salud de Ibagué.
2. Minimizar los riesgos asociados con el manejo y procesamiento de la información.
3. Garantizar el cumplimiento de las normativas de protección de datos y seguridad de la información.
4. Fomentar una cultura de seguridad entre todos los empleados, colaboradores y contratistas de la USI.
5. Definir las responsabilidades y procedimientos para el manejo seguro de la información.

3. Alcance

Este documento aplica a todos los empleados, contratistas, proveedores y terceros que manejen o tengan acceso a los sistemas de información, infraestructura tecnológica, redes y datos de la Unidad de Salud de Ibagué. Se aplica a todos los activos de información, incluidos los sistemas web, bases de datos, plataformas digitales, sistemas de gestión documental (Orfeo) y cualquier otro sistema que almacene o procese información sensible.

4. Políticas de Seguridad de la Información

4.1 Política de Confidencialidad

Toda la información manejada por la Unidad de Salud de Ibagué será tratada de manera confidencial. Solo el personal autorizado tendrá acceso a la información de acuerdo a su rol y responsabilidades. La divulgación de información a terceros se hará exclusivamente bajo autorización expresa y bajo estrictos acuerdos de confidencialidad.

4.2 Política de Integridad

La información debe ser precisa y confiable. Todos los usuarios son responsables de garantizar que los datos que procesen o manipulen se mantengan íntegros, evitando cualquier alteración no autorizada. El acceso a la modificación de datos será limitado a usuarios con permisos especiales.

4.3 Política de Disponibilidad

Los sistemas de información de la USI deben estar disponibles de manera ininterrumpida, permitiendo el acceso a la información cuando sea necesario. Se realizarán copias de seguridad periódicas y habrá redundancia en los sistemas críticos para garantizar la disponibilidad ante fallos técnicos.

4.4 Política de Protección de Datos Personales

La Unidad de Salud de Ibagué se compromete a proteger los datos personales conforme a la Ley 1581 de 2012. Se garantizará que toda recolección, almacenamiento y tratamiento de datos personales se realice con el consentimiento informado de los titulares y bajo los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

4.5 Política de Gestión de Incidentes de Seguridad

Cualquier incidente de seguridad de la información debe ser reportado inmediatamente al equipo de Seguridad de la Información. Se implementará un proceso de gestión de incidentes para responder rápida y eficazmente a cualquier violación o riesgo a la seguridad, incluyendo ataques informáticos, pérdida de información o accesos no autorizados.

4.6 Política de Acceso a la Información

El acceso a los sistemas de información será controlado mediante autenticación robusta y niveles de acceso jerárquicos. Todos los usuarios deberán utilizar credenciales personales y no compartirlas bajo ninguna circunstancia. El acceso a la información se auditará periódicamente para asegurar el cumplimiento de las políticas.

4.7 Política de Uso Aceptable de Tecnología

El uso de los recursos tecnológicos de la USI, incluidos los equipos, sistemas y redes, debe estar alineado con las políticas internas de la organización. Está prohibido utilizar estos recursos para actividades ilegales, personales o no relacionadas con las funciones laborales.

---

5. Procedimientos de Seguridad de la Información

5.1 Procedimiento de Gestión de Acceso

1. Solicitud de acceso: Cualquier solicitud de acceso a los sistemas de información debe ser autorizada por el jefe del área correspondiente.
2. Asignación de roles: Los usuarios recibirán permisos de acuerdo a sus responsabilidades, bajo el principio de mínimo privilegio.
3. Revocación de acceso: Cuando un empleado, contratista o proveedor finaliza su relación con la USI, se deberá revocar su acceso inmediatamente.

5.2 Procedimiento de Gestión de Incidentes

1. Identificación del incidente: Cualquier usuario que detecte un incidente de seguridad debe reportarlo de inmediato al área de Seguridad Informática.
2. Contención y mitigación: El equipo de seguridad evaluará el incidente y tomará medidas inmediatas para contener el impacto.
3. Análisis y resolución: Se realizará un análisis detallado para identificar las causas del incidente y se implementarán medidas correctivas.

4. Reporte final: Se emitirá un informe que detalle el incidente y las acciones correctivas implementadas.

5.3 Procedimiento de Copia de Seguridad y Recuperación

1. Frecuencia de copias de seguridad: Las copias de seguridad de los sistemas críticos se realizarán diariamente, mientras que las copias completas de la información se realizarán semanalmente.

2. Almacenamiento seguro: Las copias de seguridad se almacenarán en un lugar seguro fuera del sitio principal de operaciones y en un datacenter alterno.

3. Pruebas de restauración: Periódicamente, se realizarán pruebas de restauración para garantizar que las copias sean funcionales y se puedan recuperar en caso de fallos.

5.4 Procedimiento de Actualización de Sistemas

1. Evaluación de parches y actualizaciones: El equipo de TI revisará periódicamente las actualizaciones de seguridad de los sistemas operativos, software y hardware de la USI.

2. Aplicación de parches: Las actualizaciones críticas de seguridad se aplicarán inmediatamente. Otras actualizaciones se programarán en ventanas de mantenimiento para minimizar el impacto en las operaciones.

---

6. Responsabilidades

1. Área de Tecnología de la Información y Seguridad Informática: Responsable de implementar, monitorear y hacer cumplir las políticas de seguridad de la información.

2. Directivos y Jefes de Área: Supervisar que el personal cumpla con las políticas establecidas.

3. Personal y contratistas: Cumplir estrictamente con las políticas y procedimientos de seguridad**.**

7. Revisión y Actualización

Este documento será revisado y actualizado anualmente o cuando se presenten cambios significativos en la infraestructura tecnológica, regulaciones o amenazas a la seguridad. Las actualizaciones serán comunicadas a todo el personal de la USI.