

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESE BelloSalud

Versión: 1.0

Estado: Borrador

Responsable: Área de Sistemas

Aprobado por: Gerencia

1. Objetivo

Establecer los lineamientos para la protección de la información de la E.S.E. BelloSalud, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, mediante la adopción de controles administrativos, físicos y tecnológicos que contribuyan a la adecuada gestión de la seguridad de la información y la continuidad de los servicios institucionales.

2. Alcance

La presente política aplica a:

- Todos los servidores públicos.
- Personal de planta.
- Personal temporal.
- Contratistas.
- Prestadores de servicios.
- Pasantes.
- Proveedores con acceso a información institucional.
- Sistemas de información.
- Bases de datos.
- Equipos de cómputo.
- Correo institucional.
- Página web.
- Redes.
- Servidores.
- Información física y digital.

3. Marco Normativo

La presente política se fundamenta en:

- Constitución Política de Colombia.
- Ley 1712 de 2014.
- Ley 1581 de 2012.
- Ley 594 de 2000.
- Decreto 1078 de 2015.
- Resolución 1519 de 2020.
- Política de Gobierno Digital.
- Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC.
- Norma ISO/IEC 27001 (como referente de buenas prácticas).

4. Principios



La seguridad de la información de la E.S.E. BelloSalud se fundamenta en los siguientes principios:

Confidencialidad

La información solo podrá ser conocida por personas autorizadas.

Integridad

La información deberá mantenerse completa, exacta y protegida contra modificaciones no autorizadas.

Disponibilidad

La información estará disponible para quienes la requieran en el ejercicio de sus funciones.

Autenticidad

Toda la información deberá provenir de fuentes verificables.

Trazabilidad

Las acciones realizadas sobre la información deberán poder ser identificadas y verificadas cuando sea necesario.

5. Objetivos Específicos

La E.S.E. BelloSalud promoverá acciones orientadas a:

- Proteger la información institucional.
- Reducir riesgos de seguridad.
- Fortalecer la cultura de seguridad digital.
- Garantizar el cumplimiento normativo.
- Prevenir incidentes de seguridad.
- Proteger los datos personales de usuarios, funcionarios y terceros.
- Promover el uso adecuado de los recursos tecnológicos.

6. Roles y Responsabilidades

Gerencia

- Aprobar la presente política.
- Asignar recursos para su implementación.
- Promover el cumplimiento institucional.

Área de Sistemas

Será responsable de:

- Administrar la infraestructura tecnológica.
- Gestionar los accesos a los sistemas de información.



- Administrar servidores institucionales.
 - Implementar controles de seguridad.
 - Gestionar copias de seguridad.
 - Atender incidentes tecnológicos.
 - Proponer acciones de mejora.
-

Oficina de Comunicaciones

Será responsable de:

- Administrar el contenido publicado en el portal web institucional.
 - Velar por la correcta publicación de la información de transparencia y acceso a la información pública.
 - Coordinar la divulgación de campañas relacionadas con seguridad digital y protección de la información.
 - Apoyar la actualización de contenidos institucionales asociados al Modelo de Seguridad y Privacidad de la Información.
-

Líderes de proceso

Deberán:

- Proteger la información bajo su responsabilidad.
 - Reportar incidentes.
 - Garantizar el cumplimiento de esta política.
-

Todos los funcionarios y contratistas

Deberán:

- Hacer uso adecuado de los equipos institucionales.
 - Mantener la confidencialidad de la información.
 - No compartir usuarios ni contraseñas.
 - Reportar cualquier incidente de seguridad.
 - Cumplir las políticas institucionales relacionadas con la seguridad de la información.
-

7. Clasificación de la Información

La información institucional se clasifica en:

Información Pública

Información que puede ser divulgada libremente.

Información de Uso Interno

Información destinada exclusivamente al funcionamiento interno de la entidad.

Información Confidencial

Información cuyo acceso se limita al personal autorizado, incluyendo historias clínicas, datos personales, información financiera y demás datos protegidos por la ley.



Información Reservada

Información protegida por normas especiales o por las excepciones previstas en la legislación vigente.

8. Control de Accesos

El acceso a los sistemas de información será administrado por el Área de Sistemas, de acuerdo con las funciones y responsabilidades asignadas a cada usuario.

Los accesos serán otorgados bajo el principio de mínimo privilegio, permitiendo únicamente los permisos estrictamente necesarios para el desarrollo de las funciones.

Cuando un funcionario o contratista finalice su vínculo con la entidad, el Área de Sistemas gestionará la desactivación de los accesos institucionales correspondientes.

9. Gestión de Incidentes de Seguridad

Todo funcionario, contratista o tercero que identifique un incidente de seguridad deberá reportarlo de manera inmediata al Área de Sistemas.

La entidad documentará, analizará y gestionará los incidentes con el fin de mitigar sus efectos, evitar su recurrencia y fortalecer los controles institucionales.

10. Copias de Seguridad

La E.S.E. BelloSalud realizará copias de seguridad de la información crítica de sus sistemas de información conforme a los procedimientos establecidos por el Área de Sistemas.

Estas copias deberán protegerse contra accesos no autorizados y mantenerse disponibles para los procesos de recuperación cuando sea necesario.

Nota: Aquí dejaremos una redacción general. Más adelante, cuando revisemos con Sistemas, podremos ajustar la frecuencia (diaria, semanal o mensual) sin modificar el resto de la política.

11. Protección de Datos Personales

La E.S.E. BelloSalud garantizará el tratamiento de los datos personales conforme a la Ley 1581 de 2012 y demás normas aplicables, adoptando medidas para proteger la privacidad de los titulares de la información.

12. Capacitación y Sensibilización

La entidad promoverá actividades de capacitación y sensibilización dirigidas a servidores públicos, contratistas y demás colaboradores, con el propósito de fortalecer la cultura de seguridad y privacidad de la información.



13. Seguimiento y Mejora Continua

La implementación de esta política será objeto de seguimiento periódico por parte del Área de Sistemas, con el apoyo de las dependencias competentes, con el fin de identificar oportunidades de mejora y fortalecer la gestión de la seguridad de la información.

14. Vigencia

La presente Política de Seguridad y Privacidad de la Información rige a partir de su aprobación mediante acto administrativo expedido por la Gerencia de la E.S.E. BelloSalud y será revisada al menos una vez al año o cuando se presenten cambios normativos, tecnológicos o institucionales que así lo requieran.

