POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

BioSeryl S.A.S.

Ómica, ISO & Data Science

Política de Seguridad de la Información

POL-SGC-003

Nombre del documento:	Política de Seguridad de la Información
Tipo de documento:	Política
Código:	POL-SGC-003
Versión:	1.0
Estado:	Vigente
Fecha emisión:	Enero 2026
Normas aplicables:	ISO/IEC 27001:2022, Ley 1273 de 2009, Ley 1581 de 2012
Proceso:	Seguridad de la Información

Elaboró:	Dirección General
Revisó:	Dirección General
Aprobó:	Dirección General

Índice

1. Marco Legal 3
2. Declaración de Política de Seguridad de la Información 3
3. Objetivos de Seguridad de la Información 3
4. Alcance 4
5. Clasificación de la Información 4
6. Control de Acceso 5
6.1. Autenticación Multifactor (MFA) . . . 5
6.2. Principio de Mínimo Privilegio . . . 5
6.3. Revisión de Accesos . . . 5
6.4. Política de Contraseñas . . . 5
7. Seguridad en el Trabajo Remoto 5
7.1. Conexiones Seguras . . . 5
7.2. Seguridad de la Red Doméstica . . . 6
7.3. Bloqueo de Pantalla y Equipo . . . 6
7.4. Protección del Equipo de Trabajo . . . 6
8. Seguridad en Servicios Cloud 6
8.1. Proveedores de Nube Aprobados . . . 6
8.2. Cifrado de Datos . . . 6
8.3. Política de Respaldos en la Nube . . . 6
8.4. Acuerdos de Nivel de Servicio (SLA) . . . 7
9. Gestión de Incidentes de Seguridad 7
9.1. Clasificación de Incidentes . . . 7
9.2. Procedimiento de Respuesta . . . 7
9.3. Notificación . . . 7
10. Respaldos y Recuperación 8
10.1. Frecuencia de Respaldos . . . 8
10.2. Objetivos de Recuperación . . . 8
10.3. Pruebas de Restauración . . . 8
11. Desarrollo Seguro 8
12. Concientización y Capacitación 8
13. Revisión de la Política 9
14. Consecuencias del Incumplimiento 9
15. Control de Cambios 10

1. Marco Legal

La presente política se fundamenta en la siguiente normatividad y estándares internacionales:

- **ISO/IEC 27001:2022** — Sistema de Gestión de Seguridad de la Información (SGSI). Establece los requisitos para implementar, mantener y mejorar continuamente un SGSI, incluyendo los controles del Anexo A organizados en cuatro dominios: organizacionales, de personas, físicos y tecnológicos.
- **Ley 1273 de 2009** — Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado «*De la protección de la información y de los datos*». Tipifica los delitos informáticos en Colombia, incluyendo acceso abusivo a sistemas, interceptación de datos, suplantación de sitios web y hurto por medios informáticos.
- **Ley 1581 de 2012** — Régimen General de Protección de Datos Personales. Regula la recolección, almacenamiento, uso, circulación y supresión de datos personales, estableciendo principios de finalidad, libertad, veracidad, transparencia, acceso y seguridad.
- **Decreto 1377 de 2013** — Reglamenta parcialmente la Ley 1581 de 2012 en materia de autorización, políticas de tratamiento de datos personales y transferencias internacionales.
- **CONPES 3854 de 2016** — Política Nacional de Seguridad Digital. Establece el marco estratégico de ciberseguridad y ciberdefensa para Colombia, promoviendo la gestión de riesgos de seguridad digital en entidades públicas y privadas.
- **Ley 527 de 1999** — Comercio electrónico, firmas digitales y mensajes de datos. Define la validez jurídica de documentos y firmas electrónicas.

2. Declaración de Política de Seguridad de la Información

BioSeryl S.A.S., empresa dedicada a servicios de bioinformática, análisis de datos, consultoría en sistemas de gestión ISO y formación especializada, con operación 100 % remota y digital desde Santa Rosa de Cabal, Risaralda, reconoce que la información es uno de sus activos más valiosos y se compromete a:

1. Proteger la **confidencialidad, integridad y disponibilidad** de toda la información gestionada por la organización, incluyendo datos de clientes, datos bioinformáticos, código fuente y propiedad intelectual.
2. Gestionar los riesgos de seguridad de la información de manera sistemática, identificando amenazas y vulnerabilidades propias del entorno digital y del trabajo remoto.
3. Cumplir con la legislación colombiana vigente en materia de protección de datos personales, delitos informáticos y seguridad digital.
4. Promover una cultura de seguridad de la información entre todos los colaboradores, contratistas y partes interesadas.
5. Garantizar la continuidad de las operaciones digitales mediante controles preventivos, detectivos y correctivos adecuados al tamaño y naturaleza de la organización.
6. Mejorar continuamente las prácticas de seguridad de la información conforme a los cambios tecnológicos y normativos.

La dirección destinará los recursos necesarios para la implementación y mantenimiento de los controles de seguridad de la información y liderará con el ejemplo en su aplicación.

Juan Fernando Sambrano Narvaez
Dirección General
BioSeryl S.A.S. — NIT 902.032.735-4
Febrero de 2026

3. Objetivos de Seguridad de la Información

Los objetivos de seguridad de la información de BioSeryl S.A.S. son:

1. **Confidencialidad:** Asegurar que la información sea accesible únicamente a las personas autorizadas. Los datos de clientes, resultados de análisis bioinformáticos y código propietario deben protegerse contra accesos no autorizados.
2. **Integridad:** Garantizar la exactitud y completitud de la información y de los métodos de procesamiento. Los pipelines bioinformáticos y los resultados analíticos deben estar protegidos contra modificaciones no autorizadas.
3. **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso oportuno a la información y los servicios cuando lo requieran. Los servicios en la nube y los repositorios de datos deben mantener niveles adecuados de disponibilidad.
4. **Trazabilidad:** Mantener registros que permitan identificar quién accedió, modificó o eliminó información, y en qué momento.
5. **Cumplimiento:** Garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables en materia de seguridad de la información.

4. Alcance

Esta política aplica a:

- Todos los colaboradores de BioSeryl S.A.S., independientemente de su tipo de vinculación (empleados directos, contratistas, freelancers).
- Toda la información gestionada por la organización en cualquier formato digital, incluyendo:
  - Datos genómicos y resultados de análisis bioinformáticos de clientes.
  - Código fuente, scripts y pipelines de análisis.
  - Bases de datos biológicas y de referencia.
  - Datos personales de clientes, estudiantes y colaboradores.
  - Información financiera y administrativa.
  - Material de cursos y formación.
  - Documentación del sistema de gestión de calidad.
- Todos los servicios en la nube utilizados para el almacenamiento, procesamiento y transmisión de información.
- Los equipos de cómputo personales utilizados para el trabajo remoto.
- Las redes y conexiones utilizadas para acceder a los recursos de la organización.

Nota: BioSeryl S.A.S. no posee servidores físicos ni instalaciones de oficina. Toda la infraestructura tecnológica se basa en servicios en la nube, y todo el trabajo se realiza de forma remota.

5. Clasificación de la Información

Toda la información gestionada por BioSeryl S.A.S. se clasifica en los siguientes niveles, conforme al Anexo A, control A.5.12 de ISO/IEC 27001:2022:

Nivel	Descripción	Ejemplos	Controles mínimos
Pública	Información que puede ser conocida por cualquier persona sin restricción. No genera riesgo para la organización si se divulga.	Portafolio de servicios, información de contacto, contenido del sitio web	Sin restricciones especiales
Interna	Información de uso interno de la organización. Su divulgación no autorizada podría causar inconvenientes menores.	Procedimientos internos, actas de reuniones, planes de capacitación, cronogramas	Acceso restringido a colaboradores activos
Confidencial	Información cuya divulgación no autorizada podría causar daño significativo a la organización o a terceros.	Datos de clientes, resultados de análisis, código fuente de pipelines, información financiera, datos personales	Cifrado, acceso con MFA, control de acceso por rol, acuerdos de confidencialidad

Nivel	Descripción	Ejemplos	Controles mínimos
Reservada	Información altamente sensible cuya divulgación podría causar daño grave e irreparable. Acceso restringido al mínimo indispensable.	Datos genómicos de clientes, credenciales de acceso, claves de cifrado, secretos comerciales	Cifrado fuerte, acceso exclusivo por necesidad, registro de auditoría, doble factor de autenticación

Todos los colaboradores son responsables de identificar y manejar la información conforme a su nivel de clasificación. En caso de duda, se debe aplicar el nivel de protección superior.

6. Control de Acceso

Los controles de acceso a la información se rigen por los siguientes principios, alineados con los controles A.5.15 a A.5.18 y A.8.2 a A.8.5 del Anexo A de ISO/IEC 27001:2022:

6.1. Autenticación Multifactor (MFA)

- La autenticación multifactor (MFA) es **obligatoria** para el acceso a todos los sistemas y servicios en la nube utilizados por BioSeryl.
- Se acepta como segundo factor: aplicación de autenticación (TOTP), llave de seguridad física (FIDO2/U2F) o notificación push.
- No se acepta SMS como único segundo factor de autenticación.

6.2. Principio de Mínimo Privilegio

- Cada colaborador recibe únicamente los permisos estrictamente necesarios para desempeñar sus funciones.
- Los permisos de acceso administrativo se limitan al Dirección General o a quien éste designe formalmente.
- No se comparten cuentas de usuario. Cada persona utiliza credenciales individuales.

6.3. Revisión de Accesos

- Los permisos de acceso se revisan al menos cada **seis (6) meses** o cuando se presenten cambios en los roles o responsabilidades de los colaboradores.
- Al finalizar la relación contractual con un colaborador, se revocan inmediatamente todos los accesos (dentro de las 24 horas siguientes a la notificación).
- Se mantiene un registro actualizado de los accesos otorgados a cada usuario.

6.4. Política de Contraseñas

- Longitud mínima: **12 caracteres**.
- Debe incluir combinación de mayúsculas, minúsculas, números y caracteres especiales; o ser una frase de paso (*passphrase*) de al menos 4 palabras.
- Se recomienda el uso de un **gestor de contraseñas** aprobado por la organización.
- Las contraseñas no deben reutilizarse entre servicios.
- En caso de sospecha de compromiso, la contraseña debe cambiarse inmediatamente.

7. Seguridad en el Trabajo Remoto

Dado que BioSeryl opera 100 % de forma remota, los controles de seguridad para el trabajo a distancia son fundamentales. Se alinean con el control A.6.7 del Anexo A de ISO/IEC 27001:2022:

7.1. Conexiones Seguras

- El acceso a los recursos de la organización debe realizarse únicamente a través de conexiones cifradas (HTTPS, SSH, VPN).
- Está **prohibido** acceder a información clasificada como Confidencial o Reservada desde redes WiFi públicas o abiertas (cafeterías, aeropuertos, hoteles), a menos que se utilice una VPN aprobada.

- Las transferencias de archivos sensibles deben realizarse a través de canales cifrados (SFTP, servicios en la nube con cifrado en tránsito).

7.2. Seguridad de la Red Doméstica

- El router WiFi doméstico debe tener una contraseña segura y utilizar cifrado WPA3 o, como mínimo, WPA2.
- Se recomienda cambiar las credenciales predeterminadas del router y mantener su firmware actualizado.
- Se recomienda utilizar una red WiFi separada para dispositivos de trabajo, si el router lo permite.

7.3. Bloqueo de Pantalla y Equipo

- Los equipos de trabajo deben configurarse para bloquearse automáticamente tras **5 minutos** de inactividad.
- El desbloqueo debe requerir contraseña, PIN o autenticación biométrica.
- Al alejarse del equipo, el colaborador debe bloquearlo manualmente (Win+L / Ctrl+Cmd+Q).

7.4. Protección del Equipo de Trabajo

- Los equipos deben tener el sistema operativo actualizado con los últimos parches de seguridad.
- Se debe utilizar software antivirus/antimalware activo y actualizado.
- Los discos duros de los equipos portátiles deben estar cifrados (BitLocker en Windows, FileVault en macOS, LUKS en Linux).
- No se debe instalar software no autorizado o de fuentes no confiables en equipos utilizados para trabajo.

8. Seguridad en Servicios Cloud

Toda la infraestructura tecnológica de BioSeryl se basa en servicios en la nube. Los siguientes controles aplican conforme a los controles A.5.23 y A.8.26 del Anexo A de ISO/IEC 27001:2022:

8.1. Proveedores de Nube Aprobados

Solo se utilizan servicios en la nube que cumplan con los siguientes criterios:

- Certificaciones reconocidas de seguridad (ISO 27001, SOC 2 Type II, o equivalentes).
- Cifrado de datos en reposo y en tránsito.
- Disponibilidad de MFA para cuentas de usuario.
- Cumplimiento del RGPD o estándares equivalentes de protección de datos.
- Centros de datos en jurisdicciones con legislación adecuada de protección de datos.

La lista de proveedores aprobados es mantenida y revisada por el Dirección General. Cualquier nuevo servicio en la nube debe ser evaluado y aprobado antes de su uso.

8.2. Cifrado de Datos

- **En tránsito:** toda comunicación debe utilizar TLS 1.2 o superior.
- **En reposo:** los datos clasificados como Confidenciales o Reservados deben almacenarse cifrados (AES-256 o equivalente).
- Las claves de cifrado deben gestionarse de manera segura, separadas de los datos que protegen.

8.3. Política de Respaldos en la Nube

- Los datos críticos deben estar respaldados en al menos **dos ubicaciones geográficas diferentes** (regiones de nube distintas o proveedores distintos).
- La frecuencia de respaldo se define conforme a la clasificación de la información (ver Sección 10).
- Se debe verificar periódicamente la integridad de los respaldos.

8.4. Acuerdos de Nivel de Servicio (SLA)

Para los servicios críticos en la nube, se deben considerar:

- Disponibilidad mínima: 99,5 %.
- Tiempos de respuesta ante incidentes del proveedor.
- Procedimientos de notificación de brechas de seguridad.
- Condiciones de portabilidad y eliminación de datos al finalizar el servicio.

9. Gestión de Incidentes de Seguridad

BioSeryl S.A.S. establece un proceso de gestión de incidentes de seguridad de la información conforme a los controles A.5.24 a A.5.28 del Anexo A de ISO/IEC 27001:2022:

9.1. Clasificación de Incidentes

Severidad	Descripción	Ejemplo	Tiempo de respuesta
Baja	Evento que no afecta la confidencialidad, integridad ni disponibilidad de la información de forma significativa.	Correo de phishing detectado y bloqueado, intento fallido de acceso	72 horas
Media	Evento que podría comprometer información interna o afectar parcialmente la disponibilidad de los servicios.	Acceso no autorizado a información interna, indisponibilidad parcial de un servicio	24 horas
Alta	Evento que compromete información confidencial o afecta significativamente la operación.	Acceso no autorizado a datos de clientes, infección con malware en equipo de trabajo	4 horas
Crítica	Evento que compromete información reservada, datos personales masivos o impide la operación de la empresa.	Brecha de datos genómicos de clientes, ransomware, compromiso de credenciales administrativas	Inmediato (1 hora)

9.2. Procedimiento de Respuesta

1. **Detección e identificación:** Cualquier colaborador que detecte o sospeche un incidente de seguridad debe reportarlo inmediatamente al Dirección General por el canal de comunicación establecido (correo, chat seguro).
2. **Contención:** Se toman medidas inmediatas para aislar el incidente y evitar su propagación (desconectar equipos afectados, revocar accesos comprometidos, cambiar credenciales).
3. **Análisis:** Se investiga el origen, alcance e impacto del incidente. Se documentan las evidencias.
4. **Erradicación:** Se eliminan las causas del incidente (eliminar malware, corregir vulnerabilidades, restaurar desde respaldos).
5. **Recuperación:** Se restauran los servicios y datos afectados, verificando su integridad antes de reanudar la operación normal.
6. **Lecciones aprendidas:** Se documenta el incidente completo, se identifican las causas raíz y se implementan acciones correctivas para prevenir recurrencia.

9.3. Notificación

- Incidentes que involucren datos personales deben notificarse a la **Superintendencia de Industria y Comercio (SIC)** dentro de los **15 días hábiles** siguientes a su identificación, conforme a la Ley 1581 de 2012.
- Los clientes afectados deben ser notificados de manera oportuna cuando sus datos hayan sido comprometidos.
- Se mantiene un registro de todos los incidentes de seguridad, incluyendo los que fueron contenidos sin impacto.

10. Respaldos y Recuperación

La estrategia de respaldos de BioSeryl S.A.S. se alinea con el control A.8.13 del Anexo A de ISO/IEC 27001:2022:

10.1. Frecuencia de Respaldos

Tipo de información	Frecuencia	Retención mínima	Método
Datos de clientes y resultados de análisis	Diaria	1 año	Respaldo automatizado en nube
Código fuente y pipelines	Continua (control de versiones)	Indefinida (historial Git)	Repositorios Git con respaldo en nube
Documentación del SGC	Semanal	3 años	Respaldo en nube
Información financiera y contable	Semanal	10 años (requisito legal)	Respaldo cifrado en nube
Configuración de servicios	Tras cada cambio	6 meses	Infraestructura como código / respaldo manual

10.2. Objetivos de Recuperación

- **RPO** (*Recovery Point Objective* — Punto máximo de pérdida de datos): **24 horas** para datos generales, **4 horas** para datos de clientes en procesamiento activo.
- **RTO** (*Recovery Time Objective* — Tiempo máximo de restauración del servicio): **48 horas** para servicios generales, **12 horas** para servicios críticos de cara al cliente.

10.3. Pruebas de Restauración

- Se realizan pruebas de restauración de respaldos al menos cada **seis (6) meses**.
- Las pruebas deben verificar la integridad y completitud de los datos restaurados.
- Los resultados de las pruebas se documentan, incluyendo el tiempo real de restauración y cualquier incidencia.

11. Desarrollo Seguro

BioSeryl desarrolla pipelines bioinformáticos, scripts de análisis de datos y herramientas internas. Las prácticas de desarrollo seguro se alinean con los controles A.8.25 a A.8.28 del Anexo A de ISO/IEC 27001:2022:

1. **Control de versiones:** Todo el código fuente se gestiona en repositorios Git con historial completo de cambios. Los commits deben incluir mensajes descriptivos.
2. **Revisión de código:** Los cambios significativos en pipelines de producción deben ser revisados antes de su despliegue, cuando el tamaño del equipo lo permita.
3. **Gestión de secretos:** Las credenciales, tokens de API y claves de acceso **nunca** deben incluirse en el código fuente. Se deben utilizar variables de entorno o gestores de secretos.
4. **Dependencias:** Las dependencias de software (paquetes de Python, R, etc.) deben mantenerse actualizadas. Se deben fijar versiones específicas en los archivos de requerimientos para garantizar reproducibilidad y seguridad.
5. **Entornos separados:** Se deben mantener entornos separados de desarrollo y producción. Los datos reales de clientes no deben utilizarse en entornos de desarrollo sin anonimización previa.
6. **Validación de entradas:** Los scripts y pipelines que procesan datos externos deben validar la integridad y formato de los datos de entrada antes de procesarlos.
7. **Registro de actividad:** Los pipelines de análisis que procesen datos sensibles deben registrar las operaciones realizadas (logs) de manera que permitan trazabilidad.

12. Concientización y Capacitación

BioSeryl S.A.S. implementa un programa de concientización y capacitación en seguridad de la información, conforme al control A.6.3 del Anexo A de ISO/IEC 27001:2022:

1. **Inducción:** Todo nuevo colaborador recibe una inducción en seguridad de la información que incluye:
   - Presentación de esta política y las obligaciones derivadas.
   - Configuración segura del equipo de trabajo (cifrado de disco, antivirus, actualizaciones).
   - Activación de MFA en todos los servicios.
   - Identificación y reporte de incidentes de seguridad.
2. **Capacitación periódica:** Se realiza al menos una (1) capacitación anual en temas de seguridad de la información, que puede incluir:
   - Reconocimiento de correos de phishing e ingeniería social.
   - Manejo seguro de contraseñas y gestores de contraseñas.
   - Seguridad en el uso de servicios en la nube.
   - Protección de datos personales y datos sensibles de clientes.
   - Novedades en amenazas y buenas prácticas de ciberseguridad.
3. **Acuerdo de confidencialidad:** Todo colaborador o contratista debe firmar un acuerdo de confidencialidad antes de acceder a información clasificada como Confidencial o Reservada.

13. Revisión de la Política

Esta política se revisa como mínimo **una (1) vez al año**. También se actualizará cuando se presenten:

- Cambios en la normatividad aplicable en materia de seguridad de la información, protección de datos personales o delitos informáticos.
- Incidentes de seguridad significativos que requieran ajustes en los controles existentes.
- Cambios en la infraestructura tecnológica, servicios en la nube o modelo de operación de la organización.
- Resultados de auditorías internas o externas.
- Cambios en los servicios ofrecidos por BioSeryl o en los tipos de datos que gestiona.

La revisión queda documentada en el **Control de Cambios** del presente documento y es aprobada por el Dirección General.

14. Consecuencias del Incumplimiento

El incumplimiento de esta política se considera una falta grave y podrá dar lugar a las siguientes consecuencias, según la gravedad de la conducta:

- **Llamado de atención:** notificación formal por escrito con compromiso de corrección inmediata, para infracciones leves o primera ocurrencia.
- **Restricción o revocación de accesos:** suspensión temporal o permanente de los privilegios de acceso a sistemas, datos o servicios en la nube.
- **Terminación del contrato:** con o sin justa causa, según la gravedad y la normativa laboral o contractual aplicable.
- **Acciones legales:** BioSeryl S.A.S. se reserva el derecho de iniciar las acciones civiles y penales correspondientes conforme a la Ley 1273 de 2009 (delitos informáticos), la Ley 1581 de 2012 (protección de datos personales) y demás normas aplicables.
- **Notificación a autoridades:** en caso de que la conducta constituya un delito informático o una violación a la protección de datos personales, se informará a la Superintendencia de Industria y Comercio y/o a las autoridades penales competentes.
- **Indemnización de perjuicios:** el infractor podrá ser obligado a resarcir los daños y perjuicios ocasionados a BioSeryl S.A.S. o a terceros.

15. Control de Cambios

Versión	Fecha	Descripción del cambio	Responsable
1.0	Enero 2026	Emisión inicial del documento	Dirección General