POLÍTICA DE USO ACEPTABLE DE RECURSOS DE TI

BioSeryl S.A.S.

Ómica, ISO & Data Science

Política de Uso Aceptable de Recursos de TI

POL-TI-001

Nombre del documento:	Política de Uso Aceptable de Recursos de TI
Tipo de documento:	Política
Código:	POL-TI-001
Versión:	1.0
Estado:	Vigente
Fecha emisión:	Enero 2026
Normas aplicables:	ISO/IEC 27001:2022, Ley 1273 de 2009, Ley 1581 de 2012
Proceso:	Tecnología de la Información

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

Índice

1. Marco Normativo

La presente política se fundamenta en el marco jurídico colombiano e internacional aplicable a la seguridad de la información y el uso de tecnologías de la información:

Norma	Descripción
ISO/IEC 27001:2022	Estándar internacional para sistemas de gestión de seguridad de la información (SGSI). Establece los requisitos para implementar, mantener y mejorar continuamente la protección de los activos de información, incluyendo el control de uso aceptable de los recursos tecnológicos (Anexo A, Control A.5.10).
Ley 1273 de 2009	Ley de delitos informáticos en Colombia. Tipifica conductas punibles relacionadas con la protección de la información y de los datos, incluyendo acceso abusivo a sistemas informáticos, interceptación de datos, daño informático y uso de software malicioso.
Ley 1581 de 2012	Régimen general de protección de datos personales en Colombia. Establece los principios y obligaciones para el tratamiento de datos personales, así como los derechos de los titulares.
Decreto 1377 de 2013	Reglamentario de la Ley 1581 de 2012. Detalla las condiciones para la recolección, almacenamiento, uso, circulación y supresión de datos personales.
Ley 527 de 1999	Define y reglamenta el acceso y uso de mensajes de datos, comercio electrónico y firmas digitales en Colombia.
Ley 603 de 2000	Establece la obligación de las empresas de informar sobre el cumplimiento de normas de propiedad intelectual, incluyendo el uso de software legalmente adquirido.
Ley 1915 de 2018	Modernización del régimen de derechos de autor. Aplica al uso de software, contenidos digitales y licenciamiento en entornos tecnológicos.

BioSeryl S.A.S., como empresa 100 % digital y remota, reconoce que la totalidad de sus operaciones depende de los recursos de tecnologías de la información. Por esta razón, el uso responsable, seguro y ético de dichos recursos es una condición fundamental para la continuidad del negocio y la protección de la información de clientes, colaboradores y aliados.

2. Declaración de Política

BioSeryl S.A.S. proporciona y gestiona recursos de tecnologías de la información — cuentas corporativas, servicios en la nube, plataformas de comunicación, entornos de desarrollo, herramientas de análisis de datos y repositorios de código— con el propósito de facilitar la ejecución eficiente, segura y profesional de las actividades empresariales.

En virtud de lo anterior, BioSeryl declara su compromiso de:

a) **Garantizar** que los recursos de TI sean utilizados de manera responsable, ética y conforme a la legislación vigente.

b) **Proteger** la confidencialidad, integridad y disponibilidad de la información procesada, almacenada y transmitida a través de sus recursos tecnológicos.

c) **Establecer** reglas claras sobre el uso aceptable y prohibido de los recursos de TI, adaptadas a la realidad de una operación 100 % remota.

d) **Promover** una cultura de seguridad de la información entre todos los colaboradores, basada en la conciencia, la responsabilidad individual y la mejora continua.

e) **Preservar** la confianza de los clientes y aliados mediante la gestión adecuada de sus datos e información.

3. Alcance

3.1. Sujetos

Esta política es de obligatorio cumplimiento para todas las personas que tengan acceso a los recursos de TI de BioSeryl S.A.S., en cualquiera de las siguientes modalidades:

- **Empleados:** Personas vinculadas mediante contrato laboral, independientemente de su modalidad.
- **Contratistas:** Personas naturales o jurídicas vinculadas mediante contrato de prestación de servicios.
- **Estudiantes:** Participantes de los programas de educación informal que utilicen recursos proporcionados por BioSeryl.
- **Pasantes y practicantes:** Personas vinculadas mediante convenios de práctica o pasantía.
- **Colaboradores externos:** Consultores, asesores y aliados estratégicos con acceso a recursos tecnológicos de la empresa.

3.2. Recursos cubiertos

La política aplica a todos los recursos de TI proporcionados, gestionados o contratados por BioSeryl, incluyendo pero no limitándose a:

- **Cuentas corporativas:** Correo electrónico, plataformas de colaboración (Google Workspace, Microsoft 365 u otros que se adopten).
- **Servicios en la nube:** Almacenamiento (Google Drive, OneDrive), plataformas de cómputo, bases de datos.
- **Herramientas de desarrollo:** Entornos de desarrollo integrados, repositorios de código (GitHub, GitLab), pipelines CI/CD.
- **Plataformas de comunicación:** Chat corporativo, videoconferencias (Google Meet, Zoom, Teams, Slack u otros).
- **Herramientas de análisis:** Software estadístico, plataformas bioinformáticas, herramientas de visualización de datos.
- **Herramientas de gestión:** Sistemas de gestión de proyectos, seguimiento de tareas, CRM.
- **Dominios y presencia digital:** Sitio web corporativo, redes sociales institucionales, plataformas educativas.
- **Licencias de software:** Cualquier software adquirido o suscrito por BioSeryl para uso de sus colaboradores.

4. Definiciones

Término	Definición
Recurso de TI	Cualquier activo tecnológico — hardware, software, cuenta, servicio, plataforma o infraestructura digital— proporcionado, gestionado o contratado por BioSeryl para el desarrollo de sus actividades.
Uso aceptable	Utilización de los recursos de TI conforme a los fines empresariales para los cuales fueron provistos, dentro de los límites establecidos en esta política y la legislación vigente.
Información confidencial	Toda información no pública de BioSeryl, sus clientes o aliados, incluyendo datos técnicos, financieros, comerciales, de clientes, código fuente, metodologías y cualquier información sujeta a acuerdos de confidencialidad.
Datos personales	Cualquier información vinculada o que pueda vincularse a una persona natural identificada o identificable, conforme a la Ley 1581 de 2012.

Término	Definición
Autenticación multifactor (MFA)	Método de verificación de identidad que requiere la presentación de dos o más factores de autenticación independientes (algo que se sabe, algo que se tiene, algo que se es).
BYOD	*Bring Your Own Device.* Práctica por la cual los colaboradores utilizan sus dispositivos personales para realizar actividades laborales.
Incidente de seguridad	Evento o serie de eventos de seguridad de la información que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Servicios SaaS	*Software as a Service.* Aplicaciones de software alojadas en la nube y accesibles a través de internet, contratadas bajo modelo de suscripción.

5. Uso Aceptable

Los recursos de TI de BioSeryl están destinados principalmente al desarrollo de las actividades empresariales. Se consideran prácticas de uso aceptable:

1. **Uso con fines empresariales:** Los recursos de TI deben utilizarse primordialmente para las actividades laborales, incluyendo la ejecución de proyectos, la comunicación profesional, la investigación técnica, el desarrollo de software, el análisis de datos, la preparación de material educativo y las demás funciones inherentes al cargo o contrato.

2. **Uso personal razonable:** Se permite un uso personal moderado de los recursos de TI (por ejemplo, consulta de correo personal, noticias), siempre y cuando:

   - No interfiera con las responsabilidades laborales ni con la productividad.
   - No genere costos adicionales para la empresa.
   - No comprometa la seguridad de la información.
   - No contravenga ninguna disposición de esta política ni la legislación vigente.

3. **Respeto por licencias y derechos de autor:** Todos los colaboradores deben garantizar que el uso de software, contenido digital y cualquier recurso protegido por derechos de autor se realice de conformidad con las licencias aplicables y las disposiciones de la Política de Propiedad Intelectual (POL-PI-001).

4. **Estándares de comunicación profesional:** Toda comunicación realizada a través de los recursos de TI de BioSeryl debe mantener un tono profesional, respetuoso y cortés, que refleje los valores de la empresa. Esto aplica a correo electrónico, chat corporativo, videoconferencias, redes sociales institucionales y cualquier otro canal de comunicación.

5. **Colaboración y compartición responsable:** Al compartir archivos, enlaces o información a través de los recursos de TI, los colaboradores deben verificar los permisos de acceso y asegurarse de que solo las personas autorizadas puedan acceder a la información, aplicando el principio de mínimo privilegio.

6. Uso Prohibido

Queda expresamente prohibido utilizar los recursos de TI de BioSeryl para las siguientes actividades:

1. **Actividades ilegales:** Cualquier acción que contravenga la legislación colombiana o internacional, incluyendo pero no limitándose a las conductas tipificadas en la Ley 1273 de 2009 (delitos informáticos), la distribución de material ilegal, el fraude electrónico y la suplantación de identidad.

2. **Compartir credenciales de acceso:** Está prohibido compartir, transferir o prestar contraseñas, tokens de acceso, claves API, certificados digitales o cualquier otra credencial de autenticación asignada de forma individual. Cada credencial es personal e intransferible.

3. **Instalación de software no autorizado:** No se permite instalar, descargar ni ejecutar software no aprobado en los sistemas o cuentas corporativas de BioSeryl. Esto incluye extensiones de navegador, complementos y herramientas de terceros que no hayan sido evaluados por la empresa.

4. **Uso comercial personal:** Los recursos de TI de BioSeryl no pueden utilizarse para actividades de lucro personal, emprendimientos particulares, trabajos para terceros no relacionados con la empresa ni cualquier actividad que genere un beneficio económico ajeno a BioSeryl.

5. **Almacenamiento de datos personales en cuentas corporativas:** No se permite almacenar archivos personales (fotos, documentos, música, videos u otros) en las cuentas de almacenamiento en la nube corporativas. Estas cuentas están destinadas exclusivamente a información de la empresa.

6. **Evasión de controles de seguridad:** Está prohibido intentar eludir, desactivar o modificar los controles de seguridad establecidos por BioSeryl, incluyendo configuraciones de autenticación, políticas de contraseñas, restricciones de acceso, filtros de contenido o cualquier medida de protección implementada.

7. **Uso posterior a la terminación contractual:** Una vez finalizada la relación contractual con BioSeryl — por cualquier causa—, queda prohibido acceder, utilizar o intentar acceder a los recursos de TI de la empresa. Todas las credenciales serán revocadas al momento de la terminación.

8. **Otros usos prohibidos:**

    - Envío masivo de correos no solicitados (*spam*) desde cuentas corporativas.
    - Acceso no autorizado a cuentas, archivos o sistemas de otros colaboradores.
    - Descarga o distribución de contenido ofensivo, discriminatorio, difamatorio o que atente contra la dignidad de cualquier persona.
    - Uso de los recursos de TI para acoso, intimidación o conductas contrarias a la ética empresarial.
    - Modificación, eliminación o alteración de registros, *logs* o auditorías del sistema sin autorización.

7. Cuentas y Autenticación

Dado que BioSeryl opera de forma 100 % remota, la gestión segura de cuentas y la autenticación robusta constituyen la primera línea de defensa para la protección de los recursos de TI.

7.1. Cuentas individuales

- Cada colaborador dispondrá de cuentas individuales y personales para acceder a los recursos de TI. **No se permiten cuentas compartidas** en ninguna circunstancia.
- Las cuentas se crearán utilizando el formato de nomenclatura definido por la empresa y se asociarán a la identidad verificada del colaborador.
- La creación, modificación y eliminación de cuentas será gestionada exclusivamente por el administrador de TI o el Dirección General.

7.2. Autenticación multifactor (MFA)

- La autenticación multifactor es **obligatoria** para todos los servicios que la soporten, incluyendo correo electrónico, almacenamiento en la nube, repositorios de código, herramientas de gestión y cualquier plataforma con acceso a información confidencial.
- Se aceptan como segundo factor: aplicaciones de autenticación (Google Authenticator, Microsoft Authenticator, Authy), llaves de seguridad físicas (FIDO2/WebAuthn) y notificaciones push de plataformas verificadas.
- **No se recomienda** el uso de SMS como segundo factor debido a sus vulnerabilidades conocidas (SIM swapping). Solo se aceptará SMS cuando la plataforma no ofrezca otra alternativa.

7.3. Estándares de contraseñas

Las contraseñas de acceso a los recursos de TI de BioSeryl deben cumplir con los siguientes requisitos mínimos:

- **Longitud mínima:** 12 caracteres.
- **Complejidad:** Debe incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales; se recomienda el uso de frases de contraseña (*passphrases*).
- **No reutilización:** No se permite reutilizar contraseñas entre servicios diferentes, ni reciclar contraseñas previamente empleadas.
- **No compartir:** Las contraseñas no deben escribirse en documentos, chats, correos ni compartirse verbalmente.
- **Cambio periódico:** Las contraseñas de servicios críticos deben cambiarse al menos cada 90 días o de inmediato ante sospecha de compromiso.

7.4. Gestor de contraseñas

- El uso de un gestor de contraseñas es **obligatorio** para todos los colaboradores. BioSeryl podrá recomendar o proporcionar una herramienta específica.
- El gestor de contraseñas debe protegerse con una contraseña maestra robusta y MFA habilitado.
- Está prohibido almacenar contraseñas en archivos de texto plano, hojas de cálculo, notas adhesivas u otros medios no seguros.

7.5. Tiempo de inactividad y cierre de sesión

- Los colaboradores deben bloquear la pantalla de sus dispositivos al alejarse del equipo, aun brevemente.
- Se recomienda configurar el bloqueo automático de pantalla tras un máximo de 5 minutos de inactividad.
- Al finalizar la jornada laboral, los colaboradores deben cerrar la sesión de los servicios que no requieran conexión continua.

8. Correo Electrónico y Comunicaciones

8.1. Uso profesional

- El correo electrónico corporativo y las plataformas de comunicación de BioSeryl son herramientas de trabajo y deben utilizarse con un propósito primordialmente profesional.
- Los mensajes enviados desde cuentas corporativas representan a BioSeryl. Por lo tanto, deben mantener un lenguaje profesional, claro y respetuoso.
- Se debe utilizar la firma corporativa estándar definida por la empresa en todos los correos electrónicos externos.

8.2. Prohibición de reenvío a cuentas personales

- Está **prohibido** configurar el reenvío automático de correo corporativo a cuentas de correo personales.
- No se permite copiar, trasladar ni sincronizar información corporativa a cuentas personales de correo, almacenamiento o mensajería, salvo autorización expresa de la Dirección.

8.3. Prevención de phishing e ingeniería social

- Los colaboradores deben ejercer especial precaución con correos electrónicos, mensajes o enlaces de remitentes desconocidos o sospechosos.
- Antes de hacer clic en un enlace o descargar un archivo adjunto, se debe verificar la legitimidad del remitente y la coherencia del contenido.
- Ante cualquier sospecha de phishing o ingeniería social, el colaborador debe:
  I) No abrir enlaces ni descargar archivos.
  II) Reportar el incidente al administrador de TI o al Dirección General de inmediato.
  III) No eliminar el mensaje sospechoso hasta que sea revisado.

8.4. Jerarquía de canales de comunicación

Para garantizar la eficiencia y la trazabilidad de las comunicaciones, se establece la siguiente jerarquía de uso:

1. **Comunicaciones formales y contractuales:** Correo electrónico corporativo.
2. **Coordinación de proyectos y tareas:** Plataforma de gestión de proyectos designada.
3. **Comunicación rápida y operativa:** Chat corporativo (Slack, Teams u otro autorizado).
4. **Reuniones y discusiones en tiempo real:** Videoconferencia (Google Meet, Zoom u otro autorizado).
5. **Documentación técnica y colaborativa:** Repositorios de código y documentos compartidos en la nube.

9. Almacenamiento y Manejo de Datos

9.1. Uso exclusivo de almacenamiento aprobado

- Toda la información de BioSeryl — documentos, código fuente, datos de clientes, bases de datos, informes, material educativo— debe almacenarse exclusivamente en los servicios de almacenamiento en la nube aprobados por la empresa.
- Está prohibido utilizar servicios de almacenamiento no autorizados (cuentas personales de Dropbox, Google Drive personal, memorias USB no cifradas, entre otros) para información de la empresa.

9.2. Manejo según clasificación

- La información debe manejarse de acuerdo con su nivel de clasificación (pública, interna, confidencial, restringida), según las políticas de clasificación de la información de BioSeryl.
- La información confidencial y restringida requiere controles adicionales de acceso, cifrado en tránsito y en reposo, y restricciones de compartición.

9.3. Dispositivos personales e información confidencial

- No se permite almacenar información confidencial de BioSeryl o de sus clientes en dispositivos personales fuera de los canales aprobados. Se entiende por canales aprobados las aplicaciones corporativas sincronizadas (cuya copia local se cifra y se gestiona por la empresa).
- En caso de necesidad operativa excepcional de descarga temporal de archivos a un dispositivo local, estos deben eliminarse de forma segura una vez finalizado su uso.

9.4. Eliminación de datos al finalizar la relación contractual

- Al terminar la relación contractual con BioSeryl, el colaborador debe:
  I) Entregar o transferir toda la información corporativa que obre en su poder.
  II) Eliminar de forma segura cualquier copia local de información de la empresa en sus dispositivos personales.
  III) Confirmar por escrito la eliminación de la información.
- BioSeryl revocará todos los accesos y credenciales al momento de la terminación contractual.

10. Uso de Herramientas de Inteligencia Artificial

El uso de herramientas de inteligencia artificial (IA) forma parte de las operaciones de BioSeryl y puede generar valor significativo en productividad y calidad. Sin embargo, su uso debe enmarcarse en las siguientes directrices:

10.1. Herramientas aprobadas

- BioSeryl mantendrá un listado actualizado de herramientas de IA aprobadas para uso corporativo. Este listado será comunicado a todos los colaboradores y estará disponible en la documentación interna.
- Antes de utilizar una herramienta de IA no incluida en el listado, el colaborador debe solicitar autorización al Dirección General o al administrador de TI.
- El listado de herramientas aprobadas se revisará trimestralmente y se actualizará conforme a las necesidades operativas y las evaluaciones de seguridad.

10.2. Protección de información confidencial

- Está **estrictamente prohibido** ingresar datos confidenciales de clientes, datos personales, código fuente propietario, información financiera o cualquier información clasificada como confidencial o restringida en herramientas de IA públicas o de acceso gratuito que no ofrezcan garantías contractuales de confidencialidad.
- Antes de utilizar una herramienta de IA con información sensible, se debe verificar que la herramienta cuente con políticas de privacidad adecuadas y que los datos ingresados no sean utilizados para entrenamiento del modelo ni compartidos con terceros.
- En caso de duda sobre si determinada información puede ingresarse en una herramienta de IA, se debe consultar con el Dirección General.

10.3. Revisión de resultados

- Todo contenido generado por herramientas de IA — código, textos, análisis, traducciones, informes— debe ser **revisado, validado y verificado** por el colaborador antes de ser entregado a clientes, incorporado a proyectos o publicado en nombre de BioSeryl.
- El colaborador es responsable de la calidad, precisión y corrección del contenido final, independientemente de que haya sido asistido por IA.
- Se deben verificar especialmente: precisión factual, posibles sesgos, coherencia técnica y cumplimiento de estándares de calidad de BioSeryl.

10.4. Transparencia con clientes

- Cuando la asistencia de herramientas de IA sea material en la elaboración de un entregable — es decir, cuando la IA haya contribuido de forma sustancial al resultado—, se debe informar al cliente sobre su uso.
- La forma y el nivel de detalle de la divulgación se acordarán con la Dirección y podrán adaptarse según el tipo de proyecto y las expectativas del cliente.
- El uso de IA como herramienta auxiliar (corrección ortográfica, autocompletado de código, sugerencias menores) no requiere divulgación expresa.

11. Software y Licencias

11.1. Software autorizado

- Los colaboradores solo podrán utilizar software legalmente licenciado y autorizado por BioSeryl en el desarrollo de sus actividades.
- En caso de requerir software adicional, se debe solicitar la adquisición o autorización a la Dirección, justificando la necesidad operativa.
- BioSeryl mantendrá un inventario actualizado de las licencias de software vigentes.

11.2. Software de código abierto

- El uso de software de código abierto está permitido y es parte integral de las operaciones de BioSeryl (Python, R, QIIME2, entre otros).
- El uso de bibliotecas y herramientas de código abierto debe realizarse conforme a las directrices establecidas en la Política de Propiedad Intelectual (POL-PI-001), especialmente en lo relativo al cumplimiento de las licencias de código abierto (MIT, GPL, Apache, BSD, entre otras).
- Antes de incorporar una nueva dependencia de código abierto a un proyecto de producción, se debe verificar la compatibilidad de su licencia con el proyecto y documentar su uso.

11.3. Prohibición de piratería

- Está **terminantemente prohibido** el uso, instalación, distribución o almacenamiento de software pirata, crackeado, con licencias falsificadas o adquirido de fuentes no autorizadas.
- Esta prohibición aplica tanto a los sistemas corporativos como a los dispositivos personales cuando se utilicen para actividades de BioSeryl.
- El incumplimiento de esta disposición constituye falta grave y puede acarrear consecuencias legales conforme a la Ley 603 de 2000 y la Ley 1915 de 2018.

12. Equipos Personales (BYOD)

Dado que BioSeryl opera bajo un modelo 100 % remoto y no dispone de oficina física ni infraestructura de hardware propia, los colaboradores utilizan sus dispositivos personales para el desarrollo de las actividades laborales. En consecuencia, se establecen los siguientes requisitos mínimos de seguridad:

12.1. Requisitos mínimos de seguridad

1. **Sistema operativo actualizado:** El dispositivo debe contar con un sistema operativo soportado por el fabricante, con todas las actualizaciones de seguridad instaladas. No se permite el uso de sistemas operativos fuera de soporte (*End of Life*).
2. **Software antivirus/antimalware:** El dispositivo debe contar con una solución de antivirus o antimalware activa y actualizada. En sistemas Windows, Windows Defender con protección en tiempo real activada es aceptable.
3. **Cifrado de disco:** Se requiere el cifrado completo del disco duro del dispositivo:
   - Windows: BitLocker habilitado.
   - macOS: FileVault habilitado.
   - Linux: LUKS o cifrado equivalente.
4. **Bloqueo de pantalla:** El dispositivo debe tener configurado un bloqueo de pantalla con contraseña, PIN o biometría, con activación automática tras un máximo de 5 minutos de inactividad.

5. **Firewall activado:** El firewall del sistema operativo debe estar activado y configurado para bloquear conexiones entrantes no solicitadas.
6. **Red segura:** Se recomienda el uso de redes Wi-Fi protegidas con WPA2/WPA3. Está prohibido realizar actividades con información confidencial desde redes públicas o abiertas sin el uso de una VPN aprobada.

12.2. Separación de datos personales y laborales

- Se recomienda mantener una separación clara entre los datos personales y los datos laborales en el dispositivo, ya sea mediante el uso de perfiles de usuario distintos, carpetas separadas o contenedores cifrados.
- La información corporativa en el dispositivo local debe limitarse al mínimo necesario; se privilegia el trabajo directamente en los servicios en la nube aprobados.
- BioSeryl no accederá a la información personal almacenada en los dispositivos de sus colaboradores, salvo en los casos previstos por la ley.

13. Incidentes y Reporte

13.1. Qué constituye un incidente de seguridad

Se considera incidente de seguridad cualquier evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de los recursos de TI o la información de BioSeryl, incluyendo:

- Acceso no autorizado o sospecha de acceso no autorizado a cuentas o sistemas.
- Pérdida, robo o extravío de un dispositivo con acceso a recursos de BioSeryl.
- Infección por malware, ransomware o software malicioso.
- Recepción de correos de phishing o intentos de ingeniería social.
- Divulgación accidental de información confidencial.
- Detección de actividad inusual en cuentas corporativas.
- Compromiso o sospecha de compromiso de credenciales de acceso.
- Vulnerabilidades detectadas en herramientas o sistemas utilizados.

13.2. Cómo reportar un incidente

1. **Acción inmediata:** Si el incidente está en curso (por ejemplo, acceso no autorizado activo), el colaborador debe cambiar sus credenciales de inmediato y desconectar el servicio afectado si es posible.
2. **Notificación:** Reportar el incidente al Dirección General o al administrador de TI a la mayor brevedad posible, preferiblemente dentro de las primeras **4 horas** de su detección.
3. **Canales de reporte:** El reporte puede realizarse por cualquiera de los siguientes medios:
    - Correo electrónico al Dirección General.
    - Mensaje directo en el chat corporativo.
    - Llamada telefónica en casos de urgencia extrema.
4. **Información a incluir:** El reporte debe contener, en la medida de lo posible:
    - Descripción del incidente.
    - Fecha y hora de detección.
    - Sistemas o cuentas afectadas.
    - Acciones tomadas hasta el momento.
    - Evidencia disponible (capturas de pantalla, correos sospechosos, *logs*).

13.3. Cultura de reporte sin culpa

- BioSeryl promueve una **cultura de reporte honesto y sin represalias**. El objetivo del reporte de incidentes es proteger a la empresa y a sus colaboradores, no castigar errores involuntarios.
- Ningún colaborador será sancionado por reportar de buena fe un incidente de seguridad, incluso si el incidente fue causado por un error propio.
- Lo que sí será sancionable es la **omisión deliberada** en el reporte de incidentes conocidos, ya que esto pone en riesgo a toda la organización.
- Se valora especialmente la prontitud en el reporte: un incidente detectado y reportado a tiempo puede mitigarse significativamente; un incidente ocultado puede escalar a consecuencias graves.

14. Consecuencias del Incumplimiento

El incumplimiento de las disposiciones contenidas en esta política podrá dar lugar a las siguientes medidas, las cuales se aplicarán de manera proporcional a la gravedad de la infracción y las circunstancias del caso:

- **Llamado de atención verbal o escrito:** Para infracciones leves o de primera ocurrencia, con orientación para la corrección del comportamiento.
- **Suspensión temporal de acceso:** Restricción temporal del acceso a determinados recursos de TI mientras se investiga o se corrige la situación.
- **Terminación del contrato:** Con o sin justa causa, según la gravedad de la infracción y la normativa laboral aplicable (Código Sustantivo del Trabajo).
- **Acciones legales:** BioSeryl se reserva el derecho de iniciar las acciones civiles y penales que correspondan, especialmente en casos de:
  - Delitos informáticos (Ley 1273 de 2009).
  - Violación de datos personales (Ley 1581 de 2012).
  - Infracción de derechos de autor (Ley 1915 de 2018).
- **Responsabilidad por daños:** El infractor podrá ser requerido para resarcir los daños y perjuicios ocasionados a BioSeryl, a sus clientes o a terceros como consecuencia del incumplimiento.

La determinación de la sanción aplicable corresponde al Dirección General, quien evaluará cada caso considerando la intencionalidad, la reincidencia, el impacto del incumplimiento y la cooperación del colaborador en la investigación.

15. Revisión de la Política

- Esta política será revisada como mínimo **una vez al año** o cuando se presenten cambios significativos en:
  - La legislación colombiana o internacional aplicable.
  - Las operaciones, servicios o estructura organizacional de BioSeryl.
  - Las tecnologías, herramientas o plataformas utilizadas por la empresa.
  - El panorama de amenazas de seguridad de la información.
- La revisión estará a cargo de la Dirección General, con el apoyo de asesoría especializada en seguridad de la información cuando se considere necesario.
- Las actualizaciones serán comunicadas a todos los colaboradores y se documentarán en la tabla de control de cambios.
- Todos los colaboradores deberán acusar recibo y entendimiento de las actualizaciones realizadas a la política.

16. Control de Cambios

Versión	Fecha	Descripción del cambio	Responsable
1.0	Enero 2026	Creación inicial del documento. Definición de marco normativo, uso aceptable y prohibido, cuentas y autenticación, comunicaciones, almacenamiento de datos, herramientas de IA, software y licencias, BYOD, incidentes y consecuencias.	Dirección General