

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4D SOFT S.A.S. – CALIDAPP

NIT: 901.220.269-6

Domicilio: Medellín, Antioquia, Colombia

Correo electrónico: gerencia@4d-soft.com

Teléfono: +57 316 4509919

Fecha de entrada en vigencia: [●]

Última actualización: [●]

Versión: [●]

1. OBJETO

La presente Política de Seguridad de la Información tiene como objeto establecer los principios, responsabilidades, criterios y lineamientos generales adoptados por **4D SOFT S.A.S.**, en adelante “**4D SOFT**”, para proteger la información relacionada con sus actividades empresariales y con la prestación de los servicios asociados a la plataforma tecnológica **CalidApp**.

La Política busca preservar la:

- **Confidencialidad** de la información.
- **Integridad** de la información.
- **Disponibilidad** de la información y de los servicios.
- **Autenticidad** de los accesos y operaciones.
- **Trazabilidad** de las actividades relevantes.

La seguridad de la información constituye una responsabilidad compartida entre 4D SOFT, sus colaboradores, contratistas, proveedores, Clientes y Usuarios, de acuerdo con las funciones y responsabilidades que correspondan a cada parte.

2. ALCANCE

Esta Política será aplicable a la información y recursos tecnológicos utilizados por 4D SOFT para desarrollar sus actividades y prestar los servicios de CalidApp.

Su alcance comprende, según corresponda:

- a. CalidApp.
- b. Bases de datos.
- c. Aplicaciones.
- d. Servidores e infraestructura tecnológica.
- e. Servicios en la nube.
- f. Equipos corporativos.
- g. Redes y sistemas de comunicación.
- h. Sistemas de almacenamiento.
- i. Sistemas de respaldo.
- j. Cuentas de usuarios.
- k. Credenciales.
- l. Documentación.
- m. Información de Clientes.
- n. Datos personales.
- o. Información financiera y comercial.
- p. Código fuente y propiedad intelectual.
- q. Información de colaboradores y proveedores.
- r. Registros técnicos y de auditoría.
- s. Demás activos de información bajo responsabilidad de 4D SOFT.

3. OBJETIVOS DE SEGURIDAD

4D SOFT establece como objetivos generales:

- a. Proteger la información frente a accesos no autorizados.
- b. Prevenir la pérdida, destrucción, modificación o divulgación indebida de información.

- c. Mantener mecanismos razonables de disponibilidad de los servicios.
- d. Identificar y gestionar riesgos de seguridad.
- e. Detectar y responder oportunamente ante incidentes.
- f. Promover prácticas seguras entre colaboradores y Usuarios.
- g. Cumplir las obligaciones legales y contractuales aplicables.
- h. Proteger la información de los Clientes y Usuarios.
- i. Reducir el impacto potencial de incidentes de seguridad.
- j. Promover la mejora continua de los controles de seguridad.

4. PRINCIPIOS DE SEGURIDAD

La gestión de seguridad de la información de 4D SOFT se fundamentará, entre otros, en los siguientes principios:

4.1. Confidencialidad

La información deberá ser accesible únicamente por personas, sistemas o entidades que cuenten con autorización.

4.2. Integridad

Se deberán implementar controles destinados a prevenir modificaciones no autorizadas o indebidas de la información.

4.3. Disponibilidad

4D SOFT procurará mantener disponibles los sistemas y la información necesarios para la prestación de sus servicios, de acuerdo con las capacidades técnicas y condiciones contratadas.

4.4. Mínimo privilegio

Los accesos deberán otorgarse de acuerdo con las funciones y necesidades del usuario, procurando evitar privilegios superiores a los necesarios.

4.5. Necesidad de conocer

El acceso a información estará limitado, cuando corresponda, a las personas que requieran dicha información para cumplir sus funciones.

4.6. Responsabilidad

Toda persona con acceso a recursos de información será responsable de utilizarlos de manera adecuada y segura.

4.7. Trazabilidad

Cuando sea técnica y razonablemente posible, las actividades relevantes sobre sistemas e información deberán generar registros que permitan su posterior análisis.

4.8. Prevención

4D SOFT procurará identificar y gestionar riesgos antes de que se materialicen.

4.9. Mejora continua

Los controles de seguridad podrán ser revisados y actualizados de acuerdo con nuevos riesgos, tecnologías, incidentes, cambios legales y necesidades del negocio.

5. CLASIFICACIÓN DE LA INFORMACIÓN

4D SOFT podrá clasificar la información de acuerdo con su nivel de sensibilidad, criticidad y necesidad de protección.

De manera general, podrán utilizarse categorías como:

5.1. Información pública

Información que puede ser divulgada sin generar un riesgo significativo para 4D SOFT, sus Clientes o terceros.

5.2. Información interna

Información destinada principalmente al uso interno de 4D SOFT.

5.3. Información confidencial

Información cuyo acceso no autorizado podría generar perjuicios para 4D SOFT, sus Clientes, Usuarios o terceros.

5.4. Información restringida

Información que requiere controles reforzados debido a su naturaleza, sensibilidad o impacto potencial.

La clasificación específica podrá definirse mediante procedimientos internos.

6. RESPONSABILIDADES DE 4D SOFT

4D SOFT será responsable de establecer y mantener medidas razonables de seguridad de acuerdo con la naturaleza de sus servicios y los riesgos identificados.

Entre sus responsabilidades se encuentran:

- a. Definir controles de seguridad.
- b. Gestionar riesgos tecnológicos.
- c. Implementar mecanismos de control de acceso.
- d. Gestionar incidentes.
- e. Mantener mecanismos de respaldo cuando correspondan.
- f. Supervisar los recursos tecnológicos bajo su responsabilidad.
- g. Gestionar vulnerabilidades de manera razonable.
- h. Mantener actualizados los componentes tecnológicos cuando resulte necesario.
- i. Establecer procedimientos internos de seguridad.
- j. Capacitar o informar a sus colaboradores sobre las obligaciones de seguridad aplicables.
- k. Gestionar proveedores tecnológicos relevantes.
- l. Revisar periódicamente los controles implementados.

7. RESPONSABILIDADES DE LOS COLABORADORES Y CONTRATISTAS

Los colaboradores y contratistas de 4D SOFT que tengan acceso a información o sistemas deberán:

- a. Utilizar los recursos tecnológicos exclusivamente para fines autorizados.
- b. Proteger sus credenciales.
- c. No compartir contraseñas.
- d. Evitar almacenar información confidencial en medios no autorizados.
- e. Informar incidentes o sospechas de seguridad.
- f. Cumplir los procedimientos internos.
- g. Respetar las restricciones de acceso.
- h. Mantener la confidencialidad de la información.
- i. Utilizar equipos y sistemas de manera segura.
- j. Devolver o eliminar información cuando finalice su relación con 4D SOFT, de acuerdo con las instrucciones aplicables.

8. RESPONSABILIDADES DEL CLIENTE

El Cliente será responsable de implementar medidas adecuadas para proteger la información y las cuentas que administra dentro de CalidApp.

Entre otras obligaciones, deberá:

- a. Mantener seguras las credenciales.
- b. Administrar adecuadamente los Usuarios.
- c. Asignar permisos de acuerdo con las funciones.
- d. Revocar oportunamente accesos que ya no sean necesarios.
- e. Evitar compartir cuentas cuando ello represente un riesgo.
- f. Informar incidentes de seguridad.

- g. Mantener actualizada la información de contacto necesaria para comunicaciones de seguridad.
- h. Utilizar CalidApp de acuerdo con los Términos y Condiciones.
- i. Mantener bajo su responsabilidad los dispositivos utilizados para acceder a la Plataforma.
- j. Implementar medidas internas adicionales cuando la naturaleza de la información lo requiera.

9. CONTROL DE ACCESO

4D SOFT implementará mecanismos destinados a garantizar que el acceso a sistemas e información se encuentre limitado a usuarios autorizados.

Los controles podrán incluir:

- a. Usuarios individuales.
- b. Contraseñas.
- c. Autenticación adicional cuando se encuentre disponible.
- d. Roles y permisos.
- e. Control de sesiones.
- f. Restricción de privilegios.
- g. Bloqueo o desactivación de cuentas.
- h. Registros de acceso.
- i. Otros mecanismos técnicos disponibles.

Los permisos deberán asignarse procurando aplicar el principio de mínimo privilegio.

10. GESTIÓN DE CREDENCIALES

Las Credenciales deberán ser tratadas como información confidencial.

Los Usuarios deberán:

- a. Mantener sus contraseñas en secreto.

- b. No compartirlas con terceros.
- c. Evitar utilizar contraseñas fácilmente predecibles.
- d. No almacenar contraseñas en lugares inseguros.
- e. Informar inmediatamente cualquier sospecha de compromiso.

4D SOFT podrá establecer requisitos técnicos relacionados con la creación, modificación, recuperación y protección de contraseñas.

Cuando existan mecanismos adicionales de autenticación, podrán ser implementados de acuerdo con las características de cada servicio.

11. GESTIÓN DE USUARIOS

Los accesos deberán ser creados, modificados, suspendidos o eliminados de acuerdo con las necesidades de cada Usuario.

En el caso de colaboradores y contratistas de 4D SOFT, los accesos deberán ser revisados cuando:

- a. Se produzca un cambio de funciones.
- b. Se modifique el nivel de responsabilidad.
- c. Se detecte un riesgo.
- d. Finalice la relación laboral o contractual.

En el caso de Clientes, la administración de los Usuarios corresponderá principalmente al Cliente mediante las herramientas proporcionadas por CalidApp.

12. PROTECCIÓN DE BASES DE DATOS

4D SOFT implementará controles razonables destinados a proteger las bases de datos utilizadas por CalidApp.

Estos controles podrán incluir:

- a. Restricción de acceso.
- b. Autenticación.

- c. Gestión de privilegios.
- d. Registros de actividad.
- e. Copias de seguridad.
- f. Actualizaciones de seguridad.
- g. Monitoreo.
- h. Segmentación u otros controles técnicos cuando sean apropiados.

El acceso administrativo a bases de datos deberá limitarse al personal o proveedores que lo requieran para cumplir funciones autorizadas.

13. PROTECCIÓN DE LA INFRAESTRUCTURA

4D SOFT procurará mantener medidas de seguridad adecuadas sobre la infraestructura tecnológica utilizada para prestar CalidApp.

Dependiendo de la arquitectura implementada, estas medidas podrán incluir:

- a. Controles de acceso.
- b. Segmentación de infraestructura.
- c. Protección de redes.
- d. Sistemas de monitoreo.
- e. Actualizaciones de seguridad.
- f. Gestión de vulnerabilidades.
- g. Protección de servidores.
- h. Sistemas de respaldo.
- i. Mecanismos de disponibilidad.

Los detalles técnicos específicos de la infraestructura no serán divulgados públicamente cuando dicha divulgación pueda incrementar los riesgos de seguridad.

14. SEGURIDAD DE LAS COMUNICACIONES

Cuando técnicamente corresponda, 4D SOFT implementará mecanismos destinados a proteger la información durante su transmisión.

Estos podrán incluir mecanismos de cifrado, protocolos seguros de comunicación y controles de autenticación.

La configuración concreta dependerá de la arquitectura tecnológica, los proveedores utilizados y la naturaleza de cada servicio.

15. SEGURIDAD DE LOS DISPOSITIVOS

Los dispositivos utilizados por colaboradores o contratistas para acceder a información corporativa deberán mantenerse bajo condiciones razonables de seguridad.

Cuando corresponda, podrán implementarse medidas como:

- a. Contraseñas o mecanismos de autenticación.
- b. Actualizaciones de software.
- c. Protección contra software malicioso.
- d. Bloqueo automático.
- e. Cifrado.
- f. Restricciones de instalación de software.
- g. Gestión de dispositivos corporativos.

16. DESARROLLO SEGURO DE SOFTWARE

4D SOFT procurará incorporar prácticas de seguridad durante el ciclo de desarrollo y mantenimiento de CalidApp.

Estas podrán comprender:

- a. Control de versiones.
- b. Revisión de código.
- c. Gestión de cambios.
- d. Separación de ambientes.
- e. Pruebas.
- f. Corrección de vulnerabilidades.
- g. Control de dependencias.
- h. Gestión de credenciales y secretos.
- i. Restricción de acceso a repositorios.
- j. Evaluaciones técnicas cuando sean necesarias.

El nivel de aplicación de estas medidas dependerá de la naturaleza y criticidad del desarrollo.

17. GESTIÓN DE VULNERABILIDADES

4D SOFT procurará identificar, evaluar y gestionar vulnerabilidades que puedan afectar sus sistemas.

Cuando se identifique una vulnerabilidad, podrán adoptarse medidas como:

- a. Evaluación del riesgo.
- b. Aplicación de actualizaciones.
- c. Corrección del código.
- d. Modificación de configuraciones.
- e. Implementación de controles compensatorios.
- f. Monitoreo reforzado.
- g. Otras medidas apropiadas.

La prioridad de atención dependerá del nivel de riesgo, impacto potencial y exposición.

18. REGISTROS Y TRAZABILIDAD

Cuando sea técnica y razonablemente posible, CalidApp podrá generar registros relacionados con actividades relevantes, tales como:

- a. Inicio de sesión.
- b. Cierre de sesión.
- c. Cambios de permisos.
- d. Modificaciones relevantes.
- e. Acciones administrativas.
- f. Eventos de seguridad.
- g. Errores técnicos.

Los registros podrán ser utilizados para:

- Seguridad.
- Auditoría.
- Diagnóstico.
- Soporte.
- Investigación de incidentes.
- Cumplimiento de obligaciones legales.

Los períodos de conservación de estos registros dependerán de su naturaleza y de las obligaciones aplicables.

19. COPIAS DE SEGURIDAD

4D SOFT podrá implementar mecanismos de respaldo destinados a facilitar la recuperación de información ante determinados eventos.

La gestión de copias de seguridad comprenderá, según corresponda:

- a. Definición de información crítica.
- b. Programación de respaldos.
- c. Almacenamiento de copias.
- d. Controles de acceso.

- e. Conservación.
- f. Pruebas de restauración.
- g. Gestión de fallos.

Las condiciones específicas serán establecidas en la **Política de Copias de Seguridad**.

20. GESTIÓN DE INCIDENTES DE SEGURIDAD

4D SOFT establecerá procedimientos para identificar, evaluar, contener y gestionar incidentes de seguridad.

Un incidente podrá incluir, entre otros:

- a. Acceso no autorizado.
- b. Pérdida de información.
- c. Divulgación indebida.
- d. Alteración de información.
- e. Malware.
- f. Ataques informáticos.
- g. Compromiso de credenciales.
- h. Vulnerabilidades explotadas.
- i. Indisponibilidad significativa de servicios.

Los incidentes serán clasificados de acuerdo con su naturaleza e impacto.

21. NOTIFICACIÓN DE INCIDENTES

Cuando un incidente pueda afectar información de un Cliente o datos personales y exista una obligación legal o contractual de informar, 4D SOFT realizará la comunicación correspondiente de acuerdo con los procedimientos aplicables.

La información comunicada podrá incluir, según corresponda:

- a. Naturaleza del incidente.
- b. Información potencialmente afectada.
- c. Medidas adoptadas.
- d. Recomendaciones.
- e. Acciones de mitigación.
- f. Información de contacto.

La comunicación podrá estar condicionada a las circunstancias del incidente y a las obligaciones legales aplicables.

22. GESTIÓN DE PROVEEDORES

4D SOFT procurará evaluar los riesgos de seguridad asociados a proveedores que tengan acceso a información, sistemas o infraestructura crítica.

Cuando resulte apropiado, los contratos con proveedores podrán incluir obligaciones relacionadas con:

- a. Confidencialidad.
- b. Seguridad.
- c. Protección de datos.
- d. Control de acceso.
- e. Gestión de incidentes.
- f. Continuidad.
- g. Eliminación o devolución de información.
- h. Cumplimiento legal.

23. SEGURIDAD EN SERVICIOS DE TERCEROS

Cuando CalidApp utilice servicios tecnológicos externos, 4D SOFT procurará evaluar su pertinencia y los riesgos asociados.

Entre estos servicios podrán encontrarse:

- a. Infraestructura en la nube.
- b. Almacenamiento.
- c. Servicios de correo.
- d. Procesamiento de pagos.
- e. Servicios de inteligencia artificial.
- f. Monitoreo.
- g. Analítica.
- h. Servicios de autenticación.

La utilización de terceros no elimina las obligaciones que legalmente correspondan a 4D SOFT respecto de la información bajo su responsabilidad.

24. SEGURIDAD DE LA INFORMACIÓN DEL CLIENTE

4D SOFT adoptará medidas razonables para proteger la información almacenada en CalidApp.

Sin perjuicio de las obligaciones de 4D SOFT, el Cliente deberá implementar controles internos apropiados, especialmente respecto de:

- a. Usuarios.
- b. Credenciales.
- c. Roles.
- d. Permisos.
- e. Dispositivos.
- f. Información que cargue en la Plataforma.
- g. Exportaciones.

h. Compartición de información.

25. PROTECCIÓN DE DATOS PERSONALES

El tratamiento de datos personales se realizará de conformidad con la **Política de Tratamiento y Protección de Datos Personales de 4D SOFT S.A.S.**

Las medidas de seguridad aplicables a los datos personales deberán ser proporcionales a su naturaleza, sensibilidad, volumen, finalidad y nivel de riesgo.

Cuando 4D SOFT actúe como Encargado del Tratamiento por cuenta de un Cliente, se observarán las instrucciones y obligaciones contractuales y legales correspondientes.

26. RETENCIÓN Y ELIMINACIÓN DE INFORMACIÓN

La información será conservada de acuerdo con las necesidades operativas, obligaciones legales, contractuales y políticas de conservación aplicables.

Respecto de la información almacenada en CalidApp, después de la terminación del Servicio podrá aplicarse un período de conservación de hasta **cinco (5) años**, conforme a las condiciones establecidas en la Política de Almacenamiento y Conservación de Información.

Una vez cumplido el período aplicable, la información podrá ser eliminada, anonimizada o sometida al tratamiento que legalmente corresponda.

27. CONTINUIDAD DEL SERVICIO

4D SOFT procurará mantener mecanismos razonables destinados a garantizar la continuidad de CalidApp.

Estos podrán incluir:

a. Copias de seguridad.

- b. Monitoreo.
- c. Redundancia cuando corresponda.
- d. Procedimientos de recuperación.
- e. Gestión de incidentes.
- f. Planes de contingencia.

Las condiciones específicas de continuidad estarán establecidas en la **Política de Disponibilidad y Continuidad del Servicio**.

28. SEGURIDAD FÍSICA

Cuando 4D SOFT utilice infraestructura física propia, implementará medidas razonables para protegerla.

Cuando la infraestructura sea proporcionada por terceros, 4D SOFT procurará seleccionar proveedores que cuenten con controles adecuados para la naturaleza del servicio.

Los detalles sobre ubicación física de infraestructura crítica podrán mantenerse reservados por razones de seguridad.

29. CONCIENTIZACIÓN Y CAPACITACIÓN

4D SOFT promoverá entre sus colaboradores y contratistas prácticas adecuadas de seguridad de la información.

La capacitación podrá incluir temas relacionados con:

- a. Protección de credenciales.
- b. Phishing.
- c. Ingeniería social.
- d. Manejo de información confidencial.
- e. Protección de datos personales.

- f. Uso seguro de dispositivos.
- g. Gestión de incidentes.
- h. Buenas prácticas de seguridad.

30. AUDITORÍA Y REVISIÓN

4D SOFT podrá realizar revisiones periódicas de sus controles de seguridad con el objetivo de identificar oportunidades de mejora.

Las revisiones podrán incluir:

- a. Evaluación de controles.
- b. Revisión de accesos.
- c. Análisis de incidentes.
- d. Evaluación de vulnerabilidades.
- e. Revisión de proveedores.
- f. Pruebas técnicas.
- g. Revisión de procedimientos.

Cuando corresponda, podrán realizarse auditorías internas o externas.

31. GESTIÓN DE RIESGOS

4D SOFT procurará identificar y evaluar riesgos relacionados con la seguridad de la información.

Los riesgos podrán clasificarse considerando factores como:

- a. Probabilidad de ocurrencia.
- b. Impacto potencial.
- c. Criticidad del activo.
- d. Sensibilidad de la información.

e. Exposición.

f. Vulnerabilidades existentes.

De acuerdo con el resultado de la evaluación podrán implementarse medidas preventivas, correctivas o compensatorias.

32. CUMPLIMIENTO LEGAL Y CONTRACTUAL

4D SOFT procurará mantener sus prácticas de seguridad alineadas con las obligaciones legales, regulatorias y contractuales que resulten aplicables.

Las obligaciones específicas podrán variar según:

a. País.

b. Tipo de Cliente.

c. Naturaleza de la información.

d. Tipo de servicio contratado.

e. Legislación aplicable.

f. Requisitos contractuales.

33. INCUMPLIMIENTO DE LA POLÍTICA

El incumplimiento de esta Política por parte de colaboradores o contratistas podrá dar lugar a medidas administrativas, disciplinarias o contractuales de acuerdo con la gravedad de la conducta y la normativa aplicable.

En el caso de Clientes y Usuarios de CalidApp, un incumplimiento podrá generar medidas tales como:

a. Advertencias.

b. Restricción de determinadas funcionalidades.

c. Suspensión temporal.

- d. Bloqueo de cuentas.
- e. Terminación del Servicio.
- f. Acciones legales cuando corresponda.

34. EXCLUSIONES Y LIMITACIONES

La adopción de esta Política no constituye una garantía de seguridad absoluta.

Los sistemas informáticos y servicios conectados a Internet están expuestos a riesgos tecnológicos que no pueden eliminarse completamente.

4D SOFT adoptará medidas razonables y proporcionales para gestionar dichos riesgos, sin garantizar que pueda prevenir absolutamente todos los incidentes de seguridad.

35. CONFIDENCIALIDAD

Las personas que tengan acceso a información confidencial en virtud de sus funciones deberán mantener la reserva correspondiente.

Esta obligación podrá permanecer vigente incluso después de finalizar la relación laboral, contractual o comercial cuando así corresponda.

36. MODIFICACIÓN DE LA POLÍTICA

4D SOFT podrá modificar esta Política cuando resulte necesario debido a cambios:

- a. Tecnológicos.
- b. Operativos.
- c. Organizacionales.
- d. Legales.
- e. Regulatorios.
- f. De seguridad.

La versión vigente será publicada o puesta a disposición mediante los canales correspondientes.

37. VIGENCIA

La presente Política entrará en vigencia a partir de la fecha indicada en su encabezado y permanecerá vigente mientras sea aplicable a las actividades de 4D SOFT y CalidApp.

Las nuevas versiones reemplazarán las anteriores a partir de su fecha de entrada en vigencia.

38. DATOS DEL RESPONSABLE

4D SOFT S.A.S.

NIT: 901.220.269-6

Domicilio: Medellín, Antioquia, Colombia

Correo electrónico: gerencia@4d-soft.com

Teléfono: +57 316 4509919

Producto: CalidApp

Fecha de entrada en vigencia: [●]

Última actualización: [●]

Versión: [●]