Políticas de Seguridad de la Información

1. Política de Seguridad de la Información (PSI) de KAP

El **propósito de la presente política** es **definir el marco de principios, reglas y compromisos** que KAP implementa para **proteger la información asegurando su confidencialidad, integridad y disponibilidad, así como la** gestión de los riesgos asociados a la seguridad de la información..

La presente política debe ser aplicada por **la totalidad del personal de KAP**, incluyendo, pero sin limitarse a, empleados a tiempo completo, personal a tiempo parcial, consultores externos, contratistas, proveedores y cualquier socio de negocio que, en el desempeño de sus funciones, maneje, acceda o procese información propiedad de la compañía o de sus clientes.

El cumplimiento de esta política mitiga los riesgos de seguridad, protege la reputación de KAP y garantiza el cumplimiento de las obligaciones legales y reglamentarias relacionadas con la seguridad de la información, por esto:

> *KAP se compromete a preservar la confidencialidad, integridad y disponibilidad de su información, mediante la formulación de objetivos, definición de lineamientos, procedimientos, protocolos y controles con el propósito de gestionar de manera efectiva los activos de información y sus riesgos en el marco de su misión institucional. Igualmente, fomentará la formación de una cultura de seguridad y privacidad de la información, el cumplimiento del marco normativo vigente en esta materia y velará por la asignación de los recursos necesarios para la implementación de la política y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI"*

Sandra MAgaly MEndoza

Firma CEO

2. Objetivo y Alcance del SGSI

El objetivo principal del Sistema de Gestión de Seguridad de la Información (SGSI) de KAP es establecer un marco robusto y proactivo para la protección integral de la información cumpliendo los tres principios fundamentales: *Confidencialidad:* asegurar que solo el personal autorizado tenga acceso a la información. *Integridad* garantizar que la información sea exacta, completa y solo pueda ser modificada con autorización expresa. *Disponibilidad* garantizar que la información esté accesible cuando se necesita.

En este sentido se establecen los siguientes objetivos:

- Asegurar la confidencialidad, integridad y disponibilidad de los activos de información, mediante la gestión de los riesgos de seguridad de la información.
- Promover una cultura de seguridad de la información a los usuarios internos y demás personas vinculadas a KAP, a través de la implementación de programas de capacitación y concienciación.
- Asegurar el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información mediante la implementación de acciones correctivas, de mejora y planes de acción.
- Disminuir la probabilidad de materialización de los riesgos de seguridad de la información.
- Mitigar el impacto en caso de la materialización de los riesgos de seguridad de la Información

El alcance del SGSI abarca la totalidad de las operaciones, sistemas de información y recursos gestionados o utilizados por KAP, independientemente del lugar en donde se desarrolle la actividad o se almacene la información.

Los mecanismos establecidos en el SGSI cubren los activos de información identificados tales como:

- Información de procesos estratégicos misionales, de apoyo y propiedad Intelectual: Planos, diseños, metodologías, código fuente y cualquier otra información que confiera una ventaja competitiva a KAP, entre otros.
- Información Administrativa y Financiera: Registros contables, presupuestos, informes de rendimiento, datos de transacciones,

información operacional, entre otros.

- Información personal: Información de colaboradores, clientes, partners y proveedores, entre otros.
- Sistemas de Información Críticos: Servidores de producción y desarrollo, bases de datos, aplicaciones empresariales (ERP, CRM, etc.), y sistemas de correo electrónico.
- Recursos y Equipamiento:
    - Información almacenada: Datos residiendo en servidores corporativos, plataformas de almacenamiento en la nube, y equipos de trabajo (ordenadores de escritorio, portátiles y dispositivos móviles) propiedad de la empresa.
    - Redes y conectividad: La infraestructura de red interna (LAN/WAN), los puntos de acceso inalámbrico (Wi-Fi), las conexiones de acceso remoto y cualquier otra red utilizada para la transmisión o el acceso a los datos de KAP.
    - Entornos de trabajo: Tanto las oficinas físicas de KAP como los entornos de trabajo remoto (home office), donde se implementarán controles de seguridad equivalentes para mantener la continuidad y el nivel de protección de la información.

3. Seguridad de la Información: Un Modelo de Responsabilidad Compartida

La seguridad de la información en el entorno operativo de KAP Knowledge Application y sus clientes se rige por un modelo de responsabilidad compartida, donde cada parte (KAP, clientes, contratistas, proveedores) tiene roles y deberes claramente definidos para garantizar la integridad, confidencialidad y disponibilidad de los activos de información.

KAP Knowledge Application asume la responsabilidad de la seguridad **de la información a nivel de USUARIO Y COMPORTAMIENTO**, asegurando los mecanismos de interacción de los colaboradores con la información y los sistemas. Las obligaciones clave de KAP incluyen:

- **Cumplimiento de Políticas de Acceso:** Propender por el cumplimiento de procedimientos y protocolos internos y de clientes, para el acceso a la información.
- **Aplicación del Principio de Mínimo Privilegio (PoLP):** Asegurar que a

cada usuario se le otorguen solo los permisos y derechos de acceso estrictamente necesarios para desempeñar sus funciones laborales.

- **Gestión y Custodia de Activos:** Cumplir los lineamientos internos y de clientes, para la correcta gestión, uso y custodia de los activos de información asignados al personal de KAP.
- **Adherencia a Procedimientos Operativos:** Garantizar que todo el personal de KAP conozca y cumpla con todos los procedimientos operativos y de seguridad entregados por el Cliente para el manejo de la información.
- **Capacitación y Concientización:** Concienciar al personal sobre la importancia de la seguridad de la información y el cumplimiento de políticas, procedimientos y protocolos sobre la misma.
- **Provisión y Mantenimiento de Equipos:** Mantener las condiciones operativas y de seguridad de los equipos que KAP asigna a sus colaboradores. En el caso de equipos suministrados por el cliente, se debe asegurar que funcionarios/contratistas den el uso apropiado y lo conserven en condiciones físicas adecuadas. Así mismo debe reportar cualquier novedad u anomalía identificada en el equipo asignado.
- **Sistemas Operativos y Parches:** Garantizar que todos los sistemas operativos utilizados estén actualizados con los últimos parches de seguridad (gestión de vulnerabilidades) y configurados según las mejores prácticas de endurecimiento (*hardening*).
- **Software de Seguridad:** Implementar, mantener y gestionar las soluciones esenciales de seguridad perimetral y de *endpoint*, incluyendo:
    a. Software Antivirus/Antimalware (EPP/EDR)
    b. Mecanismos de Autenticación de Doble Factor (2FA).
- **Gestión de Derechos de Acceso:** Establecer y administrar de manera precisa los derechos de acceso a nivel de infraestructura y aplicación para cada usuario , asegurando que las directivas de seguridad se implementen correctamente a nivel técnico.

3.1. Límites de la Responsabilidad y Reporte de Incidentes

El modelo establece un límite claro para la responsabilidad de KAP:

La responsabilidad de KAP cesa en el punto de fallo de la arquitectura del cliente o en la omisión de sus responsabilidades de infraestructura.

Esto significa que si un incidente de seguridad se origina debido a una vulnerabilidad no parcheada, un *firewall* mal configurado, la falta de un sistema antivirus, o cualquier otra falla en la infraestructura o entorno de trabajo bajo la responsabilidad del cliente, KAP no será considerado responsable directo por la brecha resultante.

No obstante, es responsabilidad ineludible de KAP, el reporte al cliente de incidentes identificados.

A pesar de la delimitación de responsabilidades, KAP tiene el deber contractual y operativo de notificar de inmediato al cliente sobre cualquier incidente de seguridad, comportamiento sospechoso o vulnerabilidad detectada en los activos o entornos del cliente que sean observados durante la prestación de sus servicios. Este reporte es crucial para permitir al cliente iniciar sus procedimientos de respuesta a incidentes y mitigación de riesgos.

4. Principios de la Información

4.1. Confidencialidad

La Confidencialidad es la garantía de que la información solo es accesible por aquellos individuos, con una necesidad legítima de conocerla ('Need-to-Know').

Algunos de los mecanismos de protección son:

- **Principio de Mínimo Privilegio (PoLP):** En KAP solo se otorga al personal autorizado el acceso estrictamente necesario para el desempeño de sus funciones. Esto minimiza el riesgo de exposición de datos.
- **Gestión de Credenciales:** En KAP se han asignado usuarios y contraseñas únicas e intransferibles que deben cumplir con criterios de (longitud, complejidad y diversidad de caracteres).
- **Autenticación Reforzada:** En KAP se ha implementado el mecanismo de doble autenticación (2FA) o autenticación multifactor (MFA) en todos los sistemas y aplicaciones críticos que contienen o procesan información sensible.

4.2. Integridad

La Integridad es la garantía de aque la información, así como los medios que la procesan, almacenan o transmiten, se mantienen exactos, completos y sin modificaciones no autorizadas, sea esta intencional o accidental.

Algunos de los mecanismos de protección son:

- **Gestión de la Información Controlada:** En KAP se han Implementado lineamientos para la modificación y manipulación de datos. Todos los cambios deben ser trazables, auditables y seguir un proceso formal de aprobación y control de versiones.
- **Restricción de Almacenamiento Local:** En KAP, los respaldos y el almacenamiento de datos sensibles se realizan **exclusivamente** en los medios corporativos **autorizados**, garantizando el control, la protección y la gestión adecuada de la información. Esto indica que los colaboradores deben abstenerse de almacenar información en dispositivos locales o externos.
- **Canales Oficiales de Transferencia de Datos:** En la transferencia de información debe realizarse exclusivamente a través de los canales y sistemas corporativos autorizados y cifrados, asegurando que el tránsito de datos esté protegido contra intercepciones y modificaciones.

4.3. Disponibilidad

La Disponibilidad es la garantía de que la información y los activos del sistema que la soportan (hardware, software y redes) se encuentren operativos, accesibles y confiables cuando sean requeridos, asegurando la continuidad del servicio y minimizando las interrupciones. garantiza que los usuarios autorizados tengan acceso oportuno y confiable a la información y a los activos del sistema asociados (hardware, software, redes) cuando sea requerido, minimizando las interrupciones del servicio.

Algunos de los mecanismos de Protección son:

- **Aprovechamiento de la Nube de Google para Alta Disponibilidad:** En KAP utilizamos la infraestructura de Google Workspace y Google Cloud Platform (GCP) como habilitador principal para el almacenamiento y procesamiento de la información, garantizando un **Acuerdo de Nivel de Servicio (SLA) de 99.999%** según los términos contractuales. Esto

implica el uso de zonas de disponibilidad y mecanismos de conmutación por error (failover) automáticos gestionados por el proveedor para asegurar la continuidad del servicio incluso ante fallos regionales.

- **Estrategia de Recuperación ante Desastres (DR) y Backups Descentralizados:** En KAP Establecimos un Plan de Recuperación ante Desastres (DRP) que incluya copias de seguridad (backups) automáticas e inmutables almacenadas en ubicaciones geográficas separadas (cross-region). Esto minimiza el riesgo de pérdida de datos por fallos localizados o incidentes de ciberseguridad, asegurando una rápida reanudación de las operaciones esenciales (RTO) y una mínima pérdida de datos (RPO) crítica para la operación en remoto.
- **Adquisición de licencias en la nube para garantizar la disponibilidad del software empresarial:** En KAP mitigamos el riesgo ante fallos de disponibilidad mediante la contratación de licencias en la nube, donde el proveedor, en función de sus configuraciones internas, asegura la alta disponibilidad del software gestionado o utilizado internamente por la organización.

5. Roles y Responsabilidades

KAP ha establecido roles con responsabilidades que aseguran la estrategia, misionalidad y soporte administrativo de la organización.

Para asegurar la implementación, mantenimiento y mejora del (SGSI) de KAP, todo el personal, contratistas y socios de negocio deben conocer y cumplir las obligaciones que les correspondan en materia de seguridad de la información.

El presente apartado establece el marco de responsabilidad estructurado en dos niveles diferenciados:

1. **Roles y Responsabilidades Generales:** Delimita las obligaciones de alto nivel que corresponden a la Alta Dirección y a las estructuras centrales de seguridad (RSI), instaurando así la gobernanza y la arquitectura fundamental del SGSI.
2. **Roles y Responsabilidades Específicas:** Describe las acciones concretas y las exigencias de seguridad operativa que se esperan del personal, colaboradores y, cuando aplique, de los clientes, en su interacción cotidiana con los activos de información.

La definición precisa de estos roles asegura una respuesta unificada y eficiente ante cualquier evento o incidente de seguridad.

5.1. Generales

Responsable	Rol	Responsabilidad
KAP	Gerente General	Es el responsable máximo de la seguridad de la información y de la aprobación de las políticas y lineamientos del SGSI.
KAP	RSI (Responsable de Seguridad de la Información)	Encargado de la implementación, mantenimiento y mejora del SGSI.
KAP	Gerentes de Proyecto/Business Partners	Identificar y Formalizar al inicio del proyecto los requisitos de seguridad funcionales y no funcionales. Gestionar la solicitud de eliminación formal de accesos cuando se lleve a cabo la culminación de un proyecto o la culminación de labor de un empleado/colaborador dentro de un proyecto. Reportar cualquier pérdida o robo de información o cualquier incumplimiento de políticas de forma inmediata.
KAP	Empleados y Colaboradores	Cumplir con todas las políticas y responsabilidades de seguridad establecidas y divulgadas y generar el reporte inmediato de incidentes.

5.2. Específicos

Responsable	Área de Responsabilidad	Definición y Alcance
Empleados / Colaboradores KAP	Cultura de Seguridad	Asegurar que la información confidencial (documentos o notas) no permanezca expuesta. Bloquear siempre que sea posible la estación de trabajo al ausentarse, independientemente de que sea solo por un momento.

		Reportar inmediatamente cualquier actividad o evento sospechoso (ej. phishing, malware, accesos no autorizados). Es indispensable realizar la verificación de identidad de una persona, antes de compartir información.
RSI (Responsable de Seguridad de la Información)	Cumplimiento de Políticas de Acceso	Definición de criterios para la generación de contraseñas robustas y únicas con renovación periódica (cada 90 días o según cliente).
Empleados / Colaboradores KAP	Uso Personal e Intransferible	Asegurar que los usuarios, claves y equipos sean de uso personal e intransferible.
Empleados / Colaboradores KAP	Principio de Mínimo Privilegio	Si el equipo fue entregado por el cliente, el colaborador debe garantizar que el equipo solo cuente con los accesos requeridos para sus funciones, en caso de identificar alguna novedad respecto a este punto, deberá notificarla a su líder inmediato.
Empleados / Colaboradores KAP	Uso Exclusivo del Equipo	Si el equipo fue entregado por el cliente, el uso del equipo es exclusivamente para tareas relacionadas con el proyecto del cliente.
Empleados / Colaboradores KAP	Gestión y Almacenamiento de Información	Almacenar la información únicamente en el repositorio definido por el cliente y no generar respaldos locales ni externos.
Empleados / Colaboradores KAP	Transferencia de datos confidenciales	Realizar la transferencia de información bajo los mecanismos definidos por el cliente en internet (Sharepoint, Onedrive, Dropbox, Google Drive, etc.)
Empleados / Colaboradores KAP	Uso adecuado de la información	No utilizar información de la Compañía o del Cliente para fines personales o diferentes a los requeridos para el cumplimiento de funciones.
Empleados / Colaboradores KAP	Reporte de Incidentes	Reportar de manera inmediata cualquier pérdida, robo o incidente de seguridad al Gerente de Proyecto, y éste al cliente.
Empleados / Colaboradores KAP	Custodia Física del Equipo	Realizar bloqueo del equipo ante inactividad y custodia directa en trabajo remoto o viajes. Evitar golpes y exposición del equipo a condiciones que puedan poner en riesgo su buen funcionamiento y/o integridad. Evitar el uso inadecuado del equipo asignado en temas como carga de la batería, estado de la batería, pantalla y periféricos, entre otros.

Empleados / Colaboradores KAP	Devolución y Limpieza del Equipo	En caso de utilizar equipos del cliente, se deberá realizar la devolución según el procedimiento establecido y publicado por KAP y el cliente.

6. Política de Seguridad en Proyectos de KAP Knowledge Application

Esta política de seguridad es de aplicación obligatoria y vinculante para todos los roles y personas que participan directa o indirectamente en la ejecución de cualquier proyecto de KAP (Knowledge Application) y sus empresas vinculadas. Su alcance no se limita únicamente al personal interno de la compañía, sino que se extiende a todos los colaboradores que tengan acceso a los sistemas, información o recursos de los proyectos.

Específicamente, la política aplica a:

1. **Gerentes de Proyecto (Gerente de Proyecto o Business Partner):** Incluye a todos los responsables de la planificación, dirección, control y cierre de los proyectos, quienes deben asegurar la implementación y cumplimiento de esta política dentro de sus equipos y ámbitos de trabajo.
2. **Consultores:** Abarca a los profesionales especializados que brindan asesoramiento, análisis e implementación de soluciones dentro de los proyectos, independientemente de su relación contractual con KAP (empleados directos, contratistas o subcontratistas).
3. **Ingenieros:** Se refiere a todo el personal técnico, de desarrollo, infraestructura, seguridad o soporte, que participa en el diseño, construcción, mantenimiento y operación de los entregables o la infraestructura de los proyectos.
4. **Personal que participe en la ejecución de cualquier proyecto de KAP:** Esta categoría incluye a cualquier otro miembro del equipo (como analistas de negocio, personal administrativo de proyecto, testers, etc.) o tercero (proveedores, colaboradores temporales, etc.) que, por la naturaleza de sus funciones, acceda, procese o maneje información sensible o participe en actividades críticas dentro del ciclo de vida de los proyectos de la organización.

El cumplimiento de estas directrices es fundamental para garantizar la

confidencialidad, integridad y disponibilidad de la información de los proyectos y de la compañía.

6.1. Ciclo de Vida Desarrollo Seguro (S-SDLC)

El **Ciclo de Vida de Desarrollo Seguro (S-SDLC)** de KAP Knowledge Application representa un compromiso estratégico para integrar la seguridad como un componente fundamental y no negociable en cada etapa del desarrollo de software y sistemas. Este enfoque proactivo trasciende el modelo tradicional de "seguridad al final" (post-despliegue) y asegura que los riesgos sean identificados, mitigados y eliminados desde la fase de planificación, continuando a través del diseño, la codificación, las pruebas y el mantenimiento. Al adoptar el S-SDLC, KAP garantiza que los productos y servicios entregados no solo cumplan con los requisitos funcionales, sino que sean inherentemente robustos y resistentes contra las amenazas de ciberseguridad, salvaguardando así la integridad de la información del cliente y la reputación de la compañía.

Fase	Regla Clave	Actividades de Seguridad
Planificación y Requisitos	Definición de Requisitos de Seguridad: Todos los proyectos deben iniciar con la definición explícita de los requisitos de seguridad funcionales y no funcionales.	Análisis de riesgos inicial, definición de la superficie de ataque, identificación de requisitos regulatorios (ej. GDPR, PCI), definición de repositorio oficial y mecanismos de transferencia segura de datos.
Diseño	Análisis de Amenazas (Threat Modeling): Se debe realizar un análisis de amenazas formal para identificar vulnerabilidades potenciales en la arquitectura antes de escribir código.	Modelado de amenazas, revisión de la arquitectura de seguridad, uso de componentes seguros y aprobados.
Implementación (Codificación)	Adherencia a Estándares de Codificación Segura: Todo el código debe adherirse a las guías de codificación segura de la empresa (ver Sección 4).	Revisiones de código por pares enfocadas en seguridad, uso de herramientas SAST.
Pruebas y Verificación	Pruebas de Seguridad Exhaustivas: La seguridad debe ser una condición obligatoria para el despliegue, incluyendo pruebas dinámicas y	Pruebas de penetración (realizadas por terceros o equipo interno), Scanning de vulnerabilidades (DAST), pruebas de seguridad de

	penetración.	componentes.
Despliegue	Despliegue y Configuración Segura: Se debe automatizar la configuración de entornos para eliminar configuraciones inseguras por defecto.	*Hardening de servidores, gestión de secretos, revisión final de la configuración del entorno. Implementación cuando sea posible de DevSecOps.*
Mantenimiento y Respuesta	Monitoreo y Parches Continuos: Se debe establecer un proceso robusto para el monitoreo, parcheo y respuesta a incidentes de seguridad después del lanzamiento.	Gestión de vulnerabilidades, planes de respuesta a incidentes, feedback al equipo de desarrollo.

6.2. Principios de Arquitectura e Ingeniería de Sistemas Seguros

Principio de Mínimo Privilegio (PoLP): Un componente, usuario o proceso solo debe tener los permisos mínimos necesarios para realizar su tarea. Ejemplo: Un servicio web no debería tener permisos de administrador en la base de datos.

Defensa en Profundidad: Utilizar múltiples capas de controles de seguridad (ej. firewall, segmentación de red, encriptación, MFA) para que la falla de una capa no comprometa todo el sistema.

Falla Segura (Fail Securely): En caso de un fallo del sistema (ej. error de conexión a la base de datos o autenticación), el sistema debe denegar el acceso por defecto o pasar a un estado más seguro, en lugar de permitirlo o exponer información.

Economía de Mecanismos: Mantener los mecanismos de seguridad lo más simples y pequeños posible para facilitar su revisión, prueba y verificación de que funcionan correctamente.

Separación de Privilegios: Dividir una función crítica en varios pasos o roles diferentes que deben actuar conjuntamente para completarla. Ejemplo: Requiere la aprobación de dos directores para autorizar una transacción grande.

Diseño Abierto (Open Design): La seguridad del sistema no debe depender del secreto de su diseño o código (security through obscurity), sino en la robustez de sus mecanismos.

6.3. Políticas de Codificación Segura

Estas son las prácticas obligatorias que los desarrolladores de KAP deben seguir para prevenir las vulnerabilidades más comunes en el código.

A. Validación de Entradas:

- Nunca Confiar en la Entrada del Usuario: Toda entrada que provenga de una fuente externa (ej. formularios web, APIs, archivos) debe ser validada, sanitizada y/o escapada rigurosamente para prevenir ataques de inyección (SQL, Command Injection, XSS).

B. Gestión de Datos Sensibles:

- Cifrado en Reposo y en Tránsito: Cifrar siempre los datos sensibles (credenciales, información personal, secretos) tanto cuando están almacenados (en reposo) como cuando se transmiten a través de la red (en tránsito) usando protocolos como TLS/SSL.

- Manejo de Contraseñas: Las contraseñas nunca deben almacenarse en texto plano. Utilizar funciones de hashing robustas, lentas y con salt (ej. Argon2, bcrypt, scrypt), o delegarlas a un agente encriptador de secretos ya sea local o en la nube (Azure, AWS, GCP, entre otros) de manera que sea seguro su consumo y validación.

C. Manejo de Errores y Excepciones:

- Evitar la Exposición de Información: Las respuestas de error, logs y excepciones del sistema nunca deben exponer detalles internos (rutas de archivos, stacks, nombres de servidor, queries SQL) a los usuarios finales.

D. Autenticación y Autorización:

- Utilizar APIs de Seguridad Estándar: Usar las primitivas y frameworks de seguridad estándar de la plataforma (en lugar de implementar la propia lógica de autenticación/autorización).

- Restricción de Acceso: Implementar controles de autorización a nivel de función y de recurso (Access Control List - ACL) para asegurar que un usuario solo pueda acceder a los datos que le corresponden.

E. Uso de Componentes:

- Gestión de Dependencias: Monitorear y actualizar continuamente todas las librerías, frameworks y componentes de terceros utilizados en el software, eliminando aquellos que tengan vulnerabilidades conocidas (CVEs).

6.4. Gestión de Incidentes y No Conformidades

Reporte Inmediato: Toda pérdida o robo de equipo o cualquier incidente de seguridad deberá reportarse inmediatamente al Gerente de Proyecto y este, a su vez, al cliente.

Protocolo de Contención: En caso de robo o pérdida, se activará el protocolo de contención y bloqueo remoto de datos si el equipo lo permite.

Registro de auditoría

Detalles

NOMBRE DEL ARCHIVO	Políticas de Seguridad Versión 3 - Febrero_2026 Aprobada.docx - 2/3/26, 18:45.pdf
ESTADO	Firmado
MARCA DE TIEMPO DEL ESTADO	2026/03/03 15:48:38 UTC

Actividad

ENVIADA	pmo@kap-online.com **ha enviado** una solicitud de firma a: • Sandra MAgaly MEndoza (smendoza@kap-online.com)	2026/03/02 23:46:40 UTC
FIRMADO	**Firmado** por Sandra MAgaly MEndoza (smendoza@kap-online.com)	2026/03/03 15:48:38 UTC
COMPLETADO	Todos los firmantes han firmado este documento y ya se ha **completado**	2026/03/03 15:48:38 UTC

La dirección de correo indicada arriba para cada firmante puede estar asociada a una cuenta de Google. Puede ser la dirección de correo electrónico principal asociada a la cuenta o una secundaria.