POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA TERCEROS

Preparado por:	Revisado por:	**Aprobado por**
Felipe de Lara Analista de ciberseguridad	Rafaela Alcobaça Analista de Gobernanza de TI	Marcos Faria Director de Estructura de TI
Pedro Mota Analista de ciberseguridad	Fernanda Kleis Especialista en Gobernanza de TI	Luiz Fernando Borrego Director Ejecutivo de TI
	Flavia Segura Gerente de Gobernanza de TI y Seguridad de la Información	
	Lucas Correia Gerente de Seguridad Cibernética	
	Camilla Rocha Vanzella Coordinador de Suministros	
	Jéssica P. V. Ribeiro Abogado	

ÍNDICE

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

1. Objetivo

La información es uno de los elementos de negocio más importantes para el Grupo GOL y, por lo tanto, mantener su confidencialidad, integridad y disponibilidad son factores críticos para la Compañía. La **Política de Seguridad de la Información para Terceros** tiene como objetivo principal establecer directrices claras y robustas para la protección de los activos de información de la Compañía, garantizando la confidencialidad, integridad y disponibilidad de los datos bajo responsabilidad del Tercero. Esta política sirve como base para la definición de estándares, procedimientos y controles de seguridad, alineados con las mejores prácticas del mercado y la legislación aplicable, con el fin de mitigar riesgos, prevenir incidentes y asegurar el cumplimiento de los requisitos contractuales y regulatorios. Además, busca promover una cultura de seguridad de la información entre todos los involucrados, reforzando la importancia de la protección de los activos como parte integral de las operaciones y de la relación entre las Partes.

2. Alcance

Todas las empresas y personas jurídicas que establecen contratos formales con la Compañía se obligan a cumplir con los requisitos de Seguridad de la Información aquí definidos. El cumplimiento de las directrices establecidas es fundamental para la efectiva relación de asociación establecida para alcanzar niveles adecuados de protección de la información.

3. Definiciones y Abreviaturas

Compañía: GOL LINHAS AÉREAS INTELIGENTES S.A y todas sus empresas subsidiarias directas e indirectas, incluyendo, sin limitarse, a GOL LINHAS AÉREAS S.A.

Contrato: Cualquier instrumento que genere derechos y obligaciones para la Compañía, incluyendo, pero sin limitarse a: contratos, adendas, términos de

acuerdo, cartas de intención, distratos/términos de terminación, notificaciones y documentos relacionados.

Gestor del Contrato: Director, gerente ejecutivo, gerente o coordinador de la Compañía, siendo colaborador integrante del Área Requisitante responsable por la solicitud de Contrato a la Gerencia Jurídica de Contratos.

Gerencia Jurídica de Contratos: Gerencia integrante de la Dirección Jurídica de la Compañía, compuesta por el Núcleo de Control de Contratos y los Abogados.

Persona Jurídica: Designa una entidad que posee derechos y obligaciones y a la cual se atribuye personalidad jurídica, con definición legal conforme al Código Civil Brasileño.

Tercero: Un individuo, entidad, organización y/o sus representantes que tengan negocios existentes y/o pretendidos con GOL. Esto incluye proveedores, contratistas, consultores, potenciales o existentes, y socios.

4. Papéis e Responsabilidades

4.1 Director Ejecutivo de TI

- Establecer la dirección estratégica en materia de seguridad de la información y asegurar que los requisitos de seguridad estén integrados en la estrategia global de la organización;
- Disponibilizar recursos para implementar y mantener medidas de seguridad adecuadas relacionadas con la contratación de terceros;
- Garantizar que existan los recursos necesarios para la gestión de riesgos de terceros (roles, responsabilidades y herramientas definidos);
- Asumir la responsabilidad final sobre la seguridad de la información y la gestión de riesgos relacionados con terceros.

4.2 Seguridad Cibernética

- Definir las directrices de seguridad de la información para terceros, incluyendo requisitos, estándares y procedimientos a seguir;
- Evaluar las prácticas de seguridad de terceros (proveedores y contratistas) para garantizar el cumplimiento de los estándares de la organización;
- Monitorear el acceso de terceros a los sistemas y recursos de TI de la Compañía, aplicando controles adecuados;
- Investigar y responder a incidentes de seguridad relacionados con terceros;
- Asegurar que los empleados que interactúan con terceros estén debidamente capacitados en seguridad de la información;
- Identificar y evaluar los riesgos relacionados con terceros cuando sea necesario;
- Desarrollar estrategias de mitigación y proponer acciones correctivas;
- Analizar previamente y desde una perspectiva técnica las contrataciones antes de su formalización legal, evaluando cláusulas y condiciones contractuales cuando corresponda;
- Informar a la Gerencia Jurídica de Contratos sobre riesgos identificados en las contrataciones y sugerir ajustes necesarios en los contratos.

4.3 Gobernanza de TI

- Verificar el cumplimiento de políticas y estándares de seguridad de la información;
- Monitorear las prácticas de terceros en relación con las regulaciones y estándares de seguridad aplicables;
- Informar hallazgos y recomendaciones a la Dirección de TI y al equipo de Seguridad Cibernética;
- Apoyar en la revisión y publicación de este documento.

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

4.4 Gerencia Jurídica de Contratos

- Recibir y analizar jurídicamente las demandas de la Compañía, incluyendo contratos;
- Derivar cláusulas contractuales relacionadas a terceros para revisión técnica y aprobación del área de Seguridad Cibernética;
- Identificar riesgos jurídicos en contratos de terceros y someterlos a evaluación del Gestor del Contrato;
- Analizar desde la perspectiva legal los incidentes de seguridad de la información que involucren a terceros, cuando sea requerido por áreas internas;
- Redactar contratos con cláusulas de seguridad de la información siempre que el alcance lo exija;
- Derivar para evaluación técnica de Seguridad Cibernética las cláusulas existentes en contratos con socios, proveedores y clientes;
- Brindar orientación legal sobre temas de seguridad de la información cuando sea requerido.

4.5 Área Contratante de Servicios de Proveedores

- Asegurar que los requisitos de seguridad sean claramente comunicados a los terceros antes de la contratación y estén formalizados en los contratos o anexos específicos;
- En los casos en que los proveedores tengan empleados que accedan a la red interna o a los datos de la Compañía, esta área debe garantizar que todos estén capacitados conforme al Programa de Concientización y Capacitación en Seguridad de la Información de la Compañía;
- Mantener un canal de comunicación abierto y transparente con los terceros para tratar temas relacionados con la seguridad de la información.

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

4.6 Prestadores de Servicios / Proveedores / Terceros

- Son responsables de observar y seguir todas las directrices establecidas en esta Política de Seguridad de la Información para Terceros;
- Todas las actividades ejecutadas deben cumplir con la legislación vigente y con las normativas de los organismos y entidades reguladoras pertinentes respecto a la Seguridad de la Información.

4.7 Dirección de Personas y Cultura

- Realizar verificaciones de antecedentes y evaluaciones de riesgo al contratar terceros que tendrán acceso a información confidencial o a sistemas críticos;
- Gestionar la documentación y los registros relacionados con los terceros, incluyendo acuerdos y certificaciones de formación.

5. Referencias

ISO/IEC 27005:2019 – Sistemas de Gestión de Seguridad de la Información;
Manual de Soporte al Proveedor GOL (https://static.voegol.com.br/voegol/2021-07-19/manual-de-suporte-ao-fornecedor-GOL.pdf);
Guía de Directrices de Conducta de Terceros en la Relación con GOL (https://static.voegol.com.br/voegol/2021-07-19/CartilhaDiretrizesdeCondutaTerceirosnaRelacaocomaGOL.pdf);
PO-SUP-MS-001 – Política de Adquisiciones de la Compañía.

6. Consideraciones Generales

Los terceros/proveedores/prestadores de servicios deben cumplir con todos los requisitos legales aplicables en Brasil y comprometerse a seguir completamente los siguientes pilares, basados en las mejores prácticas de seguridad de la información:

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

- Gobernanza de la Seguridad de la Información
- Protección de Datos
- Gestión de Riesgos
- Gestión de Cuentas y Accesos
- Gestión de Activos
- Seguridad en las Operaciones
- Gestión de Registros y de Incidentes
- Gestión de Vulnerabilidades
- Desarrollo Seguro
- Seguridad en las Comunicaciones
- Seguridad Física
- Continuidad del Negocio y Gestión de Crisis
- Entrenamiento y Concientización

Además, se comprometen a:

- Proteger la información contra el acceso, modificación, destrucción o divulgación no autorizada, asegurando su confidencialidad;
- Garantizar que los recursos puestos a su disposición sean utilizados exclusivamente para los fines aprobados por la Compañía;
- Asegurar que los sistemas y la información bajo su responsabilidad estén debidamente protegidos;
- Mantener la continuidad del procesamiento de la información crítica para el negocio;
- Cumplir con las leyes y regulaciones relacionadas con la propiedad intelectual;
- Respetar todas las leyes que se apliquen a sus funciones y al sector de actividad de la Compañía;
- Comunicar a la Compañía cualquier incidente de seguridad de la información que afecte datos o cause impacto en GOL;

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

- Participar en el proceso de evaluación de seguridad de la información, mediante autoevaluaciones (Self-Assessment) en la fase previa a la contratación, durante el contrato o de forma periódica posterior.

7. Requisitos de Seguridad de la Información de Terceros en los Ambientes de la Compañía.

7.1.1 Acesso Lógico y Uso Aceptable

- El acceso lógico al entorno de red interno de la Compañía debe ser solicitado por el gestor responsable del contrato a través de la herramienta ITSM. La solicitud será evaluada y aprobada conforme a la necesidad, siguiendo las directrices corporativas de Seguridad de la Información y Gobernanza de TI;
- Para terceros que necesiten acceso remoto al entorno de la Compañía, el gestor responsable debe proporcionar acceso mediante un usuario único e individual con conexión a VPN, permitiendo únicamente el acceso a los recursos y entornos necesarios para el cumplimiento de sus funciones;
- Es responsabilidad del gestor informar la vigencia del contrato de prestación de servicios en el momento de la solicitud de acceso, así como solicitar su eliminación cuando ya no sea necesario;
- Los ordenadores de terceros no pueden conectarse a la red interna de la Compañía sin aprobación previa de TI, y deben estar protegidos con software antivirus/anti-malware y demás programas licenciados;
- Está prohibido acceder, descargar o distribuir cualquier contenido que infrinja derechos de autor o propiedad intelectual dentro de la red de la Compañía. Asimismo, está prohibido acceder o distribuir contenido pornográfico de cualquier naturaleza o que viole el Estatuto del Niño y del Adolescente;
- Cuando corresponda, el usuario y contraseña proporcionados al tercero son de uso exclusivo y no deben ser divulgados ni compartidos;

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

- El tercero debe mantener seguras sus credenciales de acceso, siendo responsable por cualquier uso indebido;
- Es responsabilidad de la empresa tercera comunicar cualquier desvinculación de colaboradores para que sus accesos sean eliminados del entorno de la Compañía;
- Está prohibido el uso compartido de usuarios y contraseñas entre prestadores de servicios.

7.1.2 Notificación de Incidentes de Seguridad de la Información

- Los incidentes o no conformidades relacionados con la Seguridad de la Información que sean conocidos por el tercero deben ser comunicados de forma inmediata a la Compañía o al gestor del contrato, para que este inicie el proceso formal de notificación;
- Una vez iniciado, el proceso de análisis, tratamiento y respuesta seguirá el mismo flujo utilizado para los incidentes internos de la Compañía.

7.1.3 Seguridad de Equipos

- Cada usuario es responsable de proteger los dispositivos físicos que contengan información de la Compañía y que estén bajo su custodia;
- Cada usuario debe tener conocimiento de que el uso de cualquier recurso de TI en el entorno de la Compañía, incluso si es de su propiedad personal, podrá estar sujeto a inspección siempre que la legislación local lo permita.

7.1.4 Violación de Conducta

Se consideran violaciones a esta Política, entre otras:

- Cualquier acción o situación que pueda exponer a la Compañía a pérdidas financieras, operativas o de imagen, de forma directa o indirecta, potencial o real, comprometiendo sus activos de información;
- Uso indebido de datos corporativos, divulgación no autorizada de

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

información, secretos comerciales u otros datos sin el consentimiento expreso de la Compañía;

- Uso de datos, información, equipos, software, sistemas u otros recursos tecnológicos con fines ilícitos, que puedan incluir violaciones de leyes, regulaciones internas o externas, normas éticas o exigencias de organismos reguladores;
- La omisión en comunicar de manera inmediata cualquier incumplimiento de esta Política.

8. Controles de Seguridad en el Entorno del Tercero

Al identificar la necesidad, de acuerdo con los criterios de evaluación de riesgos de información y ciberseguridad establecidos en el Procedimiento de Gestión de Riesgos de Proveedores, el área de Ciberseguridad registrará al proveedor en una herramienta de verificación de riesgos. Luego, el equipo de seguridad cibernética realizará un análisis del proveedor. Si el proveedor no alcanza el resultado mínimo requerido para brindar el servicio, será negado por el equipo de Ciberseguridad hasta que se implementen las mejoras necesarias generadas por el plan de recomendaciones de la plataforma.

8.1 Gobernanza de la Seguridad de la Información

- El tercero debe mantener una estructura de gobernanza en seguridad de la información alineada con las mejores prácticas del mercado (como ISO 27001 y NIST), garantizando el cumplimiento normativo y los requisitos contractuales establecidos por la Compañía;
- Debe existir una política formal de seguridad de la información que abarque directrices de protección de datos, clasificación de la información, control de accesos y gestión de incidentes. Esta política debe ser revisada periódicamente y comunicada a todos los colaboradores involucrados en la prestación del

servicio;

- Los terceros deben asegurar que sus empleados estén continuamente capacitados y sensibilizados sobre seguridad de la información, participando en programas educativos y campañas de concientización para reducir los riesgos frente a amenazas internas y externas.

8.2 Protección de Datos

- El tercero debe asegurar que todos los datos personales, sensibles o corporativos tratados estén en conformidad con la LGPD, GDPR y demás normativas aplicables. Esto incluye implementar medidas técnicas como cifrado, seudonimización y control de acceso basado en roles (RBAC);
- Los datos considerados críticos (por ejemplo, información de pasajeros, estrategias comerciales) deben ser almacenados exclusivamente en entornos seguros, con acceso físico y lógico restringido. La retención de datos más allá del período necesario está estrictamente prohibida, salvo autorización formal de la Compañía;
- Está prohibido que el tercero comparta, copie o transfiera datos de la Compañía a terceros no autorizados, incluso parcialmente. Cualquier excepción requiere aprobación previa y por escrito del área jurídica y de seguridad de la información de la Compañía.

8.3 Gestión de Riesgos

- El tercero debe realizar evaluaciones periódicas de riesgos en seguridad de la información sobre sus procesos y sistemas, identificando, analizando y tratando riesgos potenciales que puedan afectar la información de la Compañía;
- Los riesgos identificados que puedan comprometer la seguridad o la continuidad de las operaciones deben ser comunicados a la Compañía en un plazo máximo de 48 horas y tratados conforme a las directrices establecidas, implementando medidas correctivas y preventivas apropiadas.

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

8.4 Gestión de Cuentas y Accesos

El tercero debe tener un proceso formal de gestión de accesos que contemple:

- No permitir el uso de cuentas compartidas ni usuarios genéricos, aplicando controles como: forzar el cambio de contraseña en el primer acceso, bloqueo tras intentos fallidos y exigencia de contraseñas complejas;
- Gestión de concesión, modificación y revocación de accesos, especialmente los privilegios elevados;
- Métodos de control de acceso físico y lógico para visitantes;
- Controles de acceso remoto mediante VPN o soluciones similares en casos de trabajo remoto;
- Aplicación del principio de mínimo privilegio y segregación de funciones, garantizando que cada usuario tenga solo los permisos estrictamente necesarios;
- Monitoreo riguroso y revisión periódica de cuentas y accesos, asegurando trazabilidad y conformidad con las políticas de la Compañía.

8.5 Gestión de Activos

- Todos los activos de información utilizados deben estar inventariados, protegidos y gestionados de forma adecuada para evitar accesos no autorizados, robos o pérdidas de datos sensibles;
- Los equipos y sistemas utilizados para tratar datos de la Compañía deben contar con controles de seguridad como cifrado, protección contra malware y mecanismos de control de acceso.

8.6 Seguridad em las Operaciones

- Deben aplicarse controles de seguridad adecuados para garantizar la integridad, disponibilidad y confiabilidad de los servicios prestados, previniendo fallos y ataques cibernéticos;
- Se deben implementar y probar regularmente procesos de respaldo y

recuperación de datos para garantizar la continuidad de los servicios en caso de incidentes;

- El tercero debe mantener un proceso de respaldo periódico en los activos que almacenan información de la Compañía, minimizando la pérdida de datos ante incidentes.

8.7 Gestión de Registros e Incidentes

- El tercero debe contar con alta capacidad para proveer información y herramientas de gestión adecuadas al monitoreo de los servicios contratados;
- Debe proporcionar a la Compañía, cuando se le solicite, acceso a los recursos de gestión para monitoreo;
- Contar con equipos y herramientas dedicadas al monitoreo de capacidad y disponibilidad de sus activos, correlacionando alertas y generando tickets de incidentes de forma automatizada;
- Tener un proceso estructurado de respuesta a incidentes, con categorización, manuales de acción y procedimientos de tratamiento;
- Mantener a la Compañía permanentemente informada sobre cualquier limitación que afecte la prestación de servicios o el cumplimiento legal/regulatorio;
- Los incidentes deben reportarse en un plazo máximo de 24 horas al correo electrónico csirt@voegol.com.br, siguiendo el modelo establecido en el contrato. El tercero debe realizar un análisis de causa raíz y presentar un informe de lecciones aprendidas en un plazo de 10 días desde la resolución del incidente.

8.8 Gestión de Vulnerabilidades

- El tercero debe prevenir, detectar y mitigar vulnerabilidades que puedan derivar en incidentes en el entorno cibernético, demostrando sus mejores esfuerzos mediante procedimientos y controles como:

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

- Autenticación segura
- Cifrado
- Detección y prevención de intrusiones
- Prevención de fugas de información
- Análisis periódicos de vulnerabilidades
- Aplicación de parches de seguridad
- Hardening en servidores y estaciones de trabajo
- Protección contra software malicioso y bloqueo de aplicaciones no autorizadas
- Trazabilidad y segmentación de redes
- Mantenimiento de respaldos seguros de datos e información

- Se deben realizar pruebas de penetración (pentests) anualmente sobre los sistemas/servicios contratados por la Compañía. Los informes deben incluir evidencias de explotación, recomendaciones de corrección y las acciones de mitigación realizadas.

8.9 Desarrollo Seguro

- Si el tercero desarrolla software para la Compañía, debe aplicar prácticas de seguridad y privacidad reconocidas por el mercado, como Privacy and Security by Design y los principios de OWASP Top 10.
- También debe integrar el ciclo de vida de desarrollo seguro (S-SDLC), incluyendo pero no limitándose a:
    - Revisiones de código estático y dinámico
    - Pruebas de seguridad automatizadas en pipelines CI/CD
    - Validación de bibliotecas de terceros contra bases de datos de vulnerabilidades conocidas (ej. NVD)

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

8.10 Seguridad em las Comunicaciones

- Todas las comunicaciones electrónicas que involucren datos de la Compañía deben utilizar protocolos de cifrado robustos. Está prohibido utilizar redes públicas (como Wi-Fi sin protección) para transmitir datos sensibles;
- Las soluciones de correo electrónico deben contar con mecanismos de protección y transferencia segura;
- Cuando sea solicitado, el tercero debe informar y permitir el acceso a la Compañía sobre las medidas de seguridad aplicadas para la transmisión, almacenamiento y eliminación de datos, incluyendo procedimientos seguros de destrucción (en medios digitales o papel).

8.11 Seguridad Física

- El tercero debe asegurar que las instalaciones donde se presten los servicios cuenten con controles físicos adecuados, como control de accesos, cámaras de vigilancia y seguridad patrimonial.

8.12 Continuidad del Negocio y Gestión de Crisis

- Definir e implementar un programa de continuidad del negocio que asegure la prestación ininterrumpida de los servicios ante incidentes, incluyendo un plan de recuperación ante desastres;
- Dicho plan debe ser probado periódicamente y estar disponible para revisión por parte de la Compañía;
- En caso de crisis (por ejemplo, ataques de ransomware, desastres naturales), el tercero deberá activar inmediatamente un equipo de respuesta a crisis compuesto por representantes técnicos, legales y de comunicación para coordinar las acciones con la Compañía.

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno

8.13 Entrenamiento y Concientización

- El tercero es completamente responsable de garantizar que todos sus empleados, directores, socios y representantes reciban capacitación adecuada a través de un programa anual de concientización en Seguridad de la Información y Privacidad de Datos;
- El programa debe incluir campañas de phishing, orientación sobre ingeniería social, charlas, boletines informativos y otros materiales educativos relacionados con seguridad y privacidad;
- Los terceros que accedan o procesen datos en el entorno de la Compañía deben estar informados de esta Política y de los entrenamientos proporcionados por GOL;
- En los casos en que colaboradores del tercero trabajen directamente en la estructura de la Compañía (por ejemplo, por medio de "body shop" o asignación de recursos), deben obligatoriamente participar de los entrenamientos internos de concientización en seguridad y ciberseguridad definidos por el equipo de Seguridad Cibernética de GOL.

9 Control de Registros

N/A.

10 Control de Revisiones

Revisión	Fecha	Páginas Afectadas	Descripción de la Modificación
00	12/06/2025	Todas	Emisión inicial en español.

11 Anexos

N/A.

USUARIO: No utilice copias no utilizadas de este documento. Para ello, asegúrese de que esta sea la versión más actual en el sistema de gestión de documentos electrónicos antes de utilizarlo".

Uso interno