MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

Este documento de Medidas Técnicas y Organizativas de Seguridad (en adelante "**TOMS**" por sus siglas en inglés) forma parte integral del acuerdo al que se adjunta o en el que se incorpora por referencia. Dicho acuerdo puede ser un contrato, términos y condiciones, una orden de servicios, o cualquier otro documento contractual celebrado entre una entidad de Capgemini (la "**Compañía**") y una entidad proveedora (el "**Proveedor**"); en adelante, el "**Acuerdo**".

La seguridad en la prestación de los Servicios es de importancia fundamental para el Grupo Capgemini y constituye un requisito con el que el Proveedor se compromete a cumplir las medidas de seguridad de Capgemini definidas en este documento TOMS, y es una de las condiciones para que Capgemini acepte celebrar el Acuerdo. Este documento TOMS establece los requisitos mínimos de seguridad aplicables a cualquier Acuerdo. Los requisitos mínimos establecidos en este documento TOMS no prevalecerán sobre (i) las leyes aplicables relativas a la ciberseguridad de sistemas y datos, (ii) las mejores prácticas y estándares de ciberseguridad aplicables a los Servicios y (iii) reglas más precisas o estrictas que se acuerden contractualmente entre el Proveedor y la Compañía.

El Proveedor implementará y mantendrá las salvaguardas organizativas, físicas y técnicas adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos que recibe, mantiene, almacena, trata o transmite en nombre de la Compañía.

Como mínimo, sin limitarse a ello, el Proveedor implementará las medidas de seguridad físicas, técnicas y organizativas definidas a continuación.

1. REQUISITOS FÍSICOS, TÉCNICOS Y ADMINISTRATIVOS

1.1. Requisitos de seguridad física

El Proveedor garantiza que ha establecido y hará cumplir, durante la vigencia del Acuerdo y cualquier periodo posterior de asistencia de transición, salvaguardas de seguridad física adecuadas para proteger datos, hardware, software, redes, instalaciones y personal frente a accesos físicos no autorizados o maliciosos, acciones adversas o eventos (p. ej., picos eléctricos, temperaturas extremas, incendio, inundación, desastres naturales, allanamiento, hurto y robo, vandalismo y terrorismo) y, en particular:

- Se implementan controles adecuados de ingreso a instalaciones para que el acceso a las sedes e instalaciones del Proveedor sea monitoreado y restringido con base en el principio de "necesidad de conocer".
- Se implementan revisiones periódicas de acceso (al menos trimestrales) para el acceso a instalaciones y en caso de una brecha de seguridad.
- Se implementan mecanismos de protección física para limitar el acceso físico a sistemas e instalaciones.

1.2. Requisitos de seguridad técnica

1.2.1. Gestión de activos

El Proveedor garantiza que ha establecido y mantendrá, durante la vigencia del Acuerdo, un inventario de activos físicos y lógicos que soportan los Servicios.

1.2.1.1. Acceso lógico y autenticación

El Proveedor garantiza que ha establecido, documentado y hará cumplir en todo momento, durante la vigencia del Acuerdo:

- Una política robusta de contraseñas que exija, como mínimo, 12 caracteres, incluyendo una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- Que todo acceso remoto y/o privilegiado esté asegurado mediante Autenticación Multifactor (MFA).
- Un esquema de clasificación de la información que garantice una seguridad apropiada y adecuada, tanto física como lógica, según la clasificación del activo/medio.
- Mecanismos apropiados de autenticación y autorización de usuarios conforme al principio de "necesidad de conocer".
- Controles para restringir el acceso a los sistemas de información por parte de usuarios remotos, contratistas y proveedores.
- Administración oportuna y precisa de cuentas de usuario y gestión de autenticación.
- Revisiones de accesos privilegiados y de usuarios, al menos trimestralmente, para garantizar que el acceso siga siendo adecuado al rol de la persona. Los accesos se eliminarán de forma inmediata (en un plazo máximo de 48 horas) tras la terminación de la relación laboral.
- Procesos para garantizar la asignación de identificadores (IDs) únicos a cada persona.
- Procesos para asegurar el cambio regular de contraseñas por defecto y parámetros de seguridad en cumplimiento con estándares de la industria.
- Mecanismos para cifrar o aplicar hash a todas las contraseñas.
- Procesos auditables para revocar oportunamente el acceso de cuentas inactivas o de usuarios terminados/trasladados.
- Procesos auditables para la revisión anual de autorizaciones de acceso y la remediación de accesos excesivos.

1.2.2. Arquitectura y diseño de seguridad

El Proveedor garantiza que ha establecido, documentado y mantendrá en todo momento, durante la vigencia del Acuerdo:

- Una arquitectura de seguridad que asegure la entrega de medidas técnicas y organizativas apropiadas y el enfoque de "seguridad desde el diseño" (security by design).
- Un sistema de controles de defensa en profundidad que puede incluir firewall(s) técnicos efectivos y tecnologías de detección/prevención de intrusiones necesarias para proteger el acceso a sistemas y los Datos de la Compañía asociados.
- Procesos de diseño en capa de base de datos y aplicación que aseguren que las aplicaciones están diseñadas para proteger los Datos de la Compañía que se recopilan, procesan, usan, almacenan, acceden y transmiten a través de dichos sistemas.
- Mecanismos de seguridad, incluyendo gestión de dispositivos, seguridad de dispositivos, gestión de identidad y acceso, seguridad en la nube, seguridad de internet.

1.2.3. Gestión de sistemas/aplicaciones y redes

El Proveedor garantiza que ha establecido y mantendrá, durante la vigencia del Acuerdo y cualquier periodo posterior de asistencia de transición, e instalará siempre:

- Parches de seguridad aplicables.
- Configuraciones seguras aplicables.
- Procesos para monitorear, analizar y responder a alertas de seguridad.
- Elementos apropiados de diseño de seguridad de red y sistemas que permitan la segregación de datos. En caso de que el Proveedor opere en modo multi-tenancy, deberá implementarse segregación lógica de red y datos.
- Escaneo automático de correos electrónicos mediante software antimalware.
- Uso de software antimalware y su actualización regular.
- Procesos para mantener, gestionar y proteger regularmente el software instalado.
- Tecnología de monitoreo y registro (logging) para ayudar a detectar y prevenir intentos de acceso no autorizados a su red y equipos.
- Una prueba anual de penetración sobre sistemas y aplicaciones que hospedan Datos de la Compañía. El Proveedor acepta realizar (al menos anualmente, o en caso de un cambio mayor/remediación de incidente de seguridad) una prueba de penetración de sus sistemas que acceden o contienen Datos de la Compañía. El Proveedor remediará los hallazgos dentro de un plazo acorde con su criticidad y con respecto al impacto potencial del hallazgo. La prueba de penetración se realizará utilizando herramientas y/o servicios de evaluación de amenazas estándar de la industria.
- A solicitud escrita y sin costo adicional para la Compañía, el Proveedor entregará a la Compañía una copia del informe de prueba de penetración y cualquier documentación razonablemente solicitada que evidencie el cumplimiento de las obligaciones del Proveedor bajo este documento TOMS, en forma de las evaluaciones de riesgos de seguridad pertinentes.

1.2.4. Seguridad de datos

El Proveedor garantiza que ha establecido y hará cumplir siempre, durante la vigencia del Acuerdo, que:

- Los Datos de la Compañía en reposo están cifrados utilizando el algoritmo AES o un estándar equivalente, con una longitud mínima de clave de 256 bits.
- Los Datos de la Compañía en tránsito se cifran utilizando TLS 1.2 o superior con clave asimétrica mínima de 2048 bits.
- Los dispositivos que almacenan Datos de la Compañía no se retirarán fuera del sitio sin la autorización previa de la Compañía.
- Los Datos de la Compañía contenidos en medios serán eliminados/destruidos de forma que queden inutilizables e irrecuperables, antes de que el dispositivo se libere para su reutilización.
- Existen procesos y soluciones para prevenir la fuga de Datos de la Compañía.

1.2.5. Registros en papel

El Proveedor garantiza que ha establecido y hará cumplir siempre, durante la vigencia del Acuerdo:

- Una política de Escritorio Limpio y Pantalla Limpia, asegurando que el personal almacene de forma segura los documentos en papel cuando no estén en uso y bloquee o apague las pantallas de su computador y teléfono cuando se ausente de su puesto de trabajo.
- Que la información de la Compañía, incluidos los documentos en papel, manejada por el Proveedor sea clasificada, etiquetada, protegida y gestionada según su clasificación.

1.3. Requisitos de seguridad administrativa

Políticas y procedimientos de seguridad de la información

1.3.1. El Proveedor garantiza que:

- Ha formulado, desarrollado e implementado, y durante la vigencia del Acuerdo mantendrá, monitoreará y hará cumplir siempre, políticas y procedimientos escritos, completos y exhaustivos de seguridad de la información y, posteriormente, los mantendrá con un modelo de gobierno y función organizativa asociada (las "Políticas de Seguridad") aplicables a los sitios, actividades, personal y sistemas utilizados para desarrollar o prestar los Servicios.
- Las Políticas de Seguridad definirán medidas de seguridad físicas, organizativas y técnicas.
  - Nombrará a una persona dentro de su organización que será responsable de la implementación de las Políticas de Seguridad.
  - Las Políticas de Seguridad y su implementación serán revisadas regularmente por el Proveedor a nivel de gestión apropiado. En todo caso, el Proveedor nunca disminuirá el nivel de seguridad de los Servicios.
  - Confirma que su personal, contratistas, agentes y terceros que violen las Políticas de Seguridad estarán sujetos a acciones disciplinarias apropiadas.
- Implementará y mantendrá un sistema de gestión de seguridad de la información (ISMS) alineado con estándares internacionalmente reconocidos como ISO/IEC 27001 y con cualquier requisito legal y regulatorio asociado. El Proveedor deberá demostrar el cumplimiento mediante certificación o controles equivalentes y proporcionará evidencia de dicho cumplimiento previa solicitud. El Proveedor también garantizará que sus subcontratistas y afiliadas involucrados en la prestación de los Servicios se adhieran al mismo nivel de estándares de seguridad.

2. POLÍTICA DE RECURSOS HUMANOS

2.1. Verificaciones de antecedentes del personal del Proveedor

Antes de su incorporación, todo el personal del Proveedor involucrado en los Servicios deberá someterse a verificaciones de antecedentes (en la medida permitida por la ley local) para verificar que los empleados a los que se confíen Datos de la Compañía o acceso a sistemas de TI sean fiables y dignos de confianza.

2.2. Concientización en seguridad

- El Proveedor establecerá una cultura de seguridad dentro de su organización. El Proveedor garantizará que el personal involucrado en la prestación de los Servicios conozca la confidencialidad de los Datos de la Compañía y los requisitos establecidos en este documento TOMS. El personal del Proveedor recibirá formación en concientización de seguridad al momento de su contratación y se llevará a cabo formación de refuerzo al menos anualmente, o en caso de un incidente/evento mayor y/o de ciberseguridad.
- El Proveedor garantizará que el personal que viole las Políticas de Seguridad esté sujeto a medidas disciplinarias, incluyendo amonestaciones, suspensión y hasta (e incluyendo) terminación.

3. GESTIÓN DE RIESGOS DE TERCEROS

Para medir y gestionar adecuadamente los riesgos de ciberseguridad, el Proveedor mantendrá un programa integral de gestión de riesgos de terceros que evalúe el cumplimiento de seguridad de proveedores terceros y subprocesadores y de cualquier otro tercero utilizado para prestar los Servicios.

4. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

- El Proveedor contará con planes apropiados de continuidad del negocio y recuperación ante desastres de modo que la restauración de cualquier servicio prestado a la Compañía se realice dentro de los plazos acordados. Dichos planes serán aprobados por la alta dirección del Proveedor a un nivel equivalente a CEO o COO.
- El Proveedor recuperará y proporcionará acceso a la Compañía dentro del objetivo de tiempo de recuperación acordado ("RTO").
- El Proveedor garantizará la recuperación de los Datos de la Compañía conforme al objetivo de punto de recuperación acordado ("RPO").
- El Proveedor realizará pruebas de Recuperación ante Desastres al menos una vez al año (o cuando se realicen cambios significativos), incluyendo pruebas de recuperabilidad de copias de seguridad. Los planes de prueba se pondrán a disposición de la Compañía previa solicitud.
- Las copias de seguridad, incluidos los Datos de la Compañía, deberán tener el mismo nivel de protección que el impuesto a los datos en el entorno de producción.
- El Proveedor notificará a la Compañía cuando ocurra un desastre de acuerdo con la línea de tiempo establecida en este documento.

5. DATOS

5.1. Ubicación de datos y soberanía

- El Proveedor debe garantizar que todos los Datos de la Compañía (incluidas copias de seguridad y registros/logs) se almacenen y procesen dentro de las jurisdicciones en las que se prestan los Servicios, salvo acuerdo escrito en contrario.
- Cualquier transferencia de datos fuera de las jurisdicciones acordadas debe cumplir con las Leyes Aplicables de Protección de Datos.

5.2. Cifrado de datos

- Todos los Datos de la Compañía deben cifrarse en reposo y en tránsito utilizando cifrado sólido, actual, reconocido y seguro de estándar industrial (p. ej., AES-256, TLS 1.2 o superior).
- Las claves deben gestionarse de manera segura y, cuando aplique, deben ofrecerse opciones de claves gestionadas por el cliente (CMK) o Bring Your Own Key (BYOK).

5.3. Controles de acceso lógico

El Proveedor debe implementar controles de acceso estrictos, incluyendo:

- Acceso basado en roles, asegurando que las cuentas privilegiadas estén controladas y monitoreadas de forma más estricta.
  - Autenticación multifactor (MFA).
  - Acceso "just-in-time" (JIT) cuando sea posible.
  - Pruebas de penetración anuales por un tercero acreditado, incluso cuando los servicios sean suministrados por un proveedor externo, con resultados disponibles bajo demanda.
  - Revisiones regulares de configuraciones en la nube para asegurar buenas prácticas de seguridad.
- El acceso a sistemas y datos debe registrarse y monitorearse.

5.4. Auditoría y cumplimiento

- El Proveedor debe mantener y proporcionar informes de auditoría actuales de terceros (ej., ISO 27001, ISO 27017/ISO 27018, SOC 2 Tipo II, CSA STAR).
- La Compañía se reserva el derecho de:
  - Solicitar evidencia de cumplimiento,
  - Realizar evaluaciones o auditorías de seguridad (directamente o a través de un tercero de confianza),
  - Recibir notificación de cualquier hallazgo material de auditoría relacionado con sus servicios.

5.5. Continuidad del negocio y recuperación ante desastres (BC/DR)

- El Proveedor mantendrá planes de respaldo y recuperación de datos (BC/DR) que cubran fallas del sistema, corrupción de datos, ciberataques y desastres naturales.
- Los Objetivos de Punto de Recuperación (RPO) y de Tiempo de Recuperación (RTO) deben definirse y cumplirse conforme al Acuerdo de Niveles de Servicio (SLA) acordado en el Acuerdo.

5.6. Registro (logging) y monitoreo

- El Proveedor debe mantener registros completos de accesos, cambios y acciones administrativas.
- Los registros relacionados con el entorno de la Compañía o de su cliente deben conservarse por un mínimo de 12 meses y ponerse a disposición previa solicitud.
- La actividad anómala o sospechosa debe generar alertas e investigación de incidentes.

5.7. Gestión de incidentes y notificación de brechas

- El Proveedor deberá;
  - Mantener un plan de respuesta a incidentes.
  - Notificar a la Compañía cualquier brecha de seguridad real o sospechada dentro de las 24 horas.
  - Proporcionar un informe detallado, incluyendo impacto, alcance y acciones de mitigación, a más tardar 1 mes a partir de la fecha de la brecha real o sospechada.
  - Derecho a activar una investigación forense por terceros tras un incidente.

5.8. Subcontratación y servicios de terceros

- El Proveedor no debe involucrar subcontratistas o herramientas de terceros que accedan a Datos de la Compañía sin:
  - Aprobación previa y por escrito de la Compañía, y
  - vincularlos a obligaciones equivalentes de seguridad y confidencialidad.
- Debe mantenerse y actualizarse una lista de subcontratistas autorizados.

5.9. Portabilidad y eliminación de datos

Tras la terminación o expiración del Acuerdo:

- Todos los Datos de la Compañía deben devolverse en un formato legible por máquina.
- Los Datos de la Compañía deben eliminarse de forma segura de todos los sistemas (incluidas copias de seguridad) dentro de un plazo definido.
- Debe proporcionarse un certificado de destrucción previa solicitud.

5.10. Cumplimiento regulatorio e industrial

El Proveedor debe cumplir con todas las regulaciones y estándares de la industria aplicables, incluyendo (según corresponda):

- GDPR, NIS2, DORA
- ISO/IEC 27001, ISO/IEC 27017 (Seguridad en la Nube), ISO/IEC 27018 (Privacidad en la Nube)
- PCI DSS, HIPAA u otros requisitos sectoriales.
- Ley 1581 de 2012 y sus decretos reglamentarios.

6. NOTIFICACIÓN Y MITIGACIÓN DE INCIDENTES DE SEGURIDAD Y BRECHAS DE DATOS

El Proveedor se compromete a informar por escrito a la Compañía sobre cualquier brecha de seguridad sin demora indebida (y, en cualquier caso, dentro de las 24 horas) después de tener conocimiento de la brecha de seguridad. Además, el Proveedor proporcionará proactivamente a la Compañía cualquier información sobre la causa y las consecuencias de la brecha de seguridad, así como cualquier información adicional razonablemente solicitada por la Compañía para fines de investigación de la brecha y para permitir que la Compañía cumpla con sus obligaciones bajo la ley aplicable o requerimiento regulatorio pertinente. La información podrá proporcionarse gradualmente si no está disponible de inmediato.

En caso de cualquier brecha de seguridad, el Proveedor se compromete a remediar dicha brecha con prontitud y a mitigar cualquier efecto perjudicial derivado. De igual manera, si debido a una brecha de seguridad por parte del Proveedor la Compañía está obligada por ley aplicable o requerimiento regulatorio a notificar a las autoridades y/o a las personas afectadas, el Proveedor se compromete a reembolsar a la Compañía los costos razonables asociados con dicha notificación.

7. AUDITORÍA

El Proveedor garantiza que ha establecido y hará cumplir, durante la vigencia del Acuerdo, procedimientos para llevar a cabo evaluaciones anuales e independientes de riesgos de seguridad relacionadas con la prestación de los Servicios. El Proveedor proporcionará una copia del informe de evaluación a la Compañía previa solicitud y sin costo adicional para la Compañía. El Proveedor suministrará a la Compañía informes detallados de auditoría. Si estos informes se consideran insatisfactorios para la Compañía, la Compañía se reserva el derecho de realizar una auditoría in situ o remota con al menos treinta (30) días de aviso previo. La Compañía limitará el alcance a áreas y documentos directamente relacionados con los Servicios y con el cumplimiento del Acuerdo.

La Compañía también podrá auditar el cumplimiento de los Servicios según se establece en estas TOMS, o según se establezca en el Acuerdo, o según lo requiera la ley o una autoridad competente.

La Compañía se reserva el derecho de discontinuar o restringir la conectividad o el acceso a la información para el Proveedor en los siguientes casos:

- El Proveedor rechaza una solicitud de auditoría de seguridad realizada por la Compañía o por su auditor de seguridad independiente designado; o
- Las acciones correctivas identificadas como parte de una auditoría de seguridad o establecidas por la Compañía no se implementan.

8. ELIMINACIÓN DE LA INFORMACIÓN AL FINAL DEL CONTRATO DE APROVISIONAMIENTO

Salvo que se estipule lo contrario en un documento contractual que tenga precedencia sobre este documento TOMS y excepto en caso de obligación legal, el Proveedor deberá, sin demora indebida y dentro

de un periodo máximo de treinta (30) días siguientes a la finalización del Acuerdo, independientemente de la causa de terminación, eliminar (o devolver a la Compañía) de sus propios recursos toda la información, incluidos, entre otros, los Datos de la Compañía recibidos.

9. SUBCONTRATACIÓN

Cualquier referencia al Proveedor se entenderá que incluye al Proveedor y a sus subcontratistas. Cuando el Proveedor subcontrate los Servicios que presta a la Compañía con un tercero, deberá obtenerse la aprobación previa y por escrito de la Compañía, tal como se establece en el Acuerdo o por ley. El Proveedor confirma que, antes de contratar al tercero, debe realizarse una evaluación de riesgos de seguridad de terceros conforme a los estándares de seguridad establecidos en este documento TOMS, para demostrar la alineación del subcontratista con las medidas establecidas en este documento TOMS. Los informes de evaluación se proporcionarán a la Compañía previa solicitud. El Proveedor mantendrá un directorio de los subcontratistas que utiliza para los Servicios y proporcionará una copia de dicho directorio a la Compañía previa solicitud.