**MEDIDAS TÉCNICAS Y ORGANIZACIONALES DE SEGURIDAD**

Los Proveedores que tengan acceso a información de Capgemini o de sus clientes, incluyendo, pero no limitado a Datos Personales, deberán implementar y mantener las medidas de seguridad administrativas, físicas y técnicas pertinentes para proteger la confidencialidad, integridad y disponibilidad de la información que reciban, mantengan, almacenen, procesen o transmitan en nombre de Capgemini.

Los Proveedores deberán contar, sin limitación, con las siguientes medidas de seguridad técnicas y organizacionales durante toda la relación comercial con Capgemini:

1. **GENERALES.**

   a) El Proveedor formula, desarrolla e implementa políticas y procedimientos de seguridad de la información con una función especificada y una persona es responsable de la implementación de la seguridad de la información.
   b) El Proveedor revisa las políticas, procedimientos e implementaciones de seguridad de la información al nivel administrativo correspondiente.

2. **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.** El Proveedor debe contar con:

   a) Un programa continuo de políticas de seguridad de la información, procedimientos de seguridad y controles técnicos de seguridad.
   b) Un programa de gestión de incidentes de seguridad.
   c) Un programa de concientización sobre seguridad.
   d) Planes de continuidad y recuperación de negocios, los cuales incluyen pruebas periódicas;
   e) Procedimientos rigurosos de control de cambios.
   f) Procedimientos para llevar a cabo evaluaciones periódicas de riesgos de seguridad independientes para identificar activos de información cruciales, evaluar las amenazas a dichos activos, determinar potenciales vulnerabilidades y otorgar reparación oportuna.

3. **ACCESO Y AUTENTICACIÓN.** El Proveedor debe contar con:

   a) Mecanismos pertinentes para la autenticación y autorización de usuarios de conformidad con una política de “necesidad de conocer” respecto a los sistemas que respaldan el negocio de Capgemini.
   b) Controles para restringir el acceso a sus sistemas para usuarios remotos, contratistas y proveedores.
   c) Administración oportuna y exacta de la gestión de cuentas de usuarios y autenticación para sus sistemas.
   d) Procesos para garantizar la asignación de identificadores (ID) únicos a cada persona con acceso a computadoras.
   e) Procesos para garantizar que los valores predeterminados de contraseñas y parámetros de seguridad proporcionados por el Proveedor se cambien y gestionen de forma adecuada continuamente.
   f) Mecanismos para rastrear todo acceso a los datos por ID único.
   g) Mecanismos para encriptar o desasociar todas las contraseñas.

h) Proceso para revocar de inmediato acceso de cuentas inactivas o usuarios dados de baja/transferidos.
i) Buen procedimiento de autenticación para proteger sus puntos de conexión (equipos de escritorio y portátiles).
j) Controles para brindar protección contra los riegos de las instalaciones de informática móvil y comunicación.

4. **REGISTRO EN PAPEL**.

a) El Proveedor debe contar con una política de escritorio limpio y pantalla vacía.
b) El Proveedor deberá asegurar que la información, que incluye documentos en papel, , se clasifica, etiqueta, protege y maneja de conformidad con la política de clasificación de documentos.

5. **COMUNICACIÓN ELECTRÓNICA.** El Proveedor deberá asegurar que:

a) Se escanean automáticamente los correos electrónicos mediante software antivirus basado en el servidor.
b) El cableado de telecomunicaciones que transporte datos o respalde los servicios de información esté protegido contra intercepción o daño.

6. **ALMACENAMIENTO DE DATOS**. El Proveedor deberá asegurar que:

a) El equipo, la información o el software no se lleven fuera del sitio sin la autorización previa de Capgemini.
b) Se aplica seguridad a los equipos fuera del sitio, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
c) Se revisan todos los equipos que contengan medios de almacenamiento para garantizar que se haya eliminado o sobrescrito cualquier categoría especial de Datos Personales (es decir, Datos Personales Confidenciales) y software bajo licencia antes de la eliminación de los mismos.

7. **ACCESO DE USUARIOS LOCALES**. El Proveedor deberá asegurar que:

a) En caso de que el Proveedor esté trabajando en modo de múltiples usuarios, se implementa la separación de redes y datos.
b) El acceso físico a las instalaciones del Proveedor esté restringido al personal autorizado.
c) Se implementa la revisión periódica de acceso tanto para el acceso lógico (red) como para el acceso físico (instalaciones).

8. **CONCIENTIZACIÓN SOBRE SEGURIDAD**. El Proveedor garantiza que ha establecido y durante la relación comercial con Capgemini siempre hará cumplir que se implemente un programa de concientización sobre seguridad.

9. **CERTIFICACIÓN ISO.** El Proveedor deberá garantizar que ha establecido y durante la relación comercial con Capgemini siempre hará cumplir, que:

a) Su sistema de gestión de seguridad esté certificado o alineado con las normas ISO 27001 y SSAE16/ISAE3402.

b) Se proporcionan servicios para el negocio de Capgemini con el uso de centros de datos que cuenten con la certificación SAS 70 Tipo II o con la certificación ISO27001 (o equivalente, como mínimo).

10. **ACCESO FÍSICO.** El Proveedor debe garantizar que ha establecido y durante la relación comercial con Capgemini (incluyendo cualquier periodo de asistencia de transición "TAP") hará cumplir:

a) Mecanismos de protección física para todos los activos de información y tecnología de la información a fin de garantizar que dichos activos y tecnología estén almacenados y protegidos en centros de datos adecuados.
b) Controles pertinentes de ingreso a las instalaciones para limitar el acceso físico a los sistemas que almacenan o procesan los datos.
c) Procesos para garantizar que el acceso a las instalaciones esté monitoreado y restringido según la "necesidad de conocer".
d) Controles para proteger físicamente todos los datos y destruir de forma correcta la información.

11. **ARQUITECTURA Y DISEÑO DE SEGURIDAD**. El Proveedor deberá contar con:

a) Una arquitectura de seguridad que garantice el suministro de las medidas de seguridad técnica y organizacional pertinentes.
b) Funcionalidad que permita encriptar datos personales.
c) Un sistema de uno o más cortafuegos efectivos y tecnologías de detección de intrusión que se necesiten para proteger los datos.
d) Procesos de diseño de base de datos y capa de aplicación que garanticen que las aplicaciones estén diseñadas para proteger los datos recopilados, tratados, utilizados, almacenados, consultados y transmitidos a través de dichos sistemas.

12. **GESTIÓN DE SISTEMA Y RED.** El Proveedor debe garantizar que ha establecido y durante la relación comercial con Capgemini (incluyendo cualquier periodo de asistencia de transición "TAP") siempre implementará y mantendrá:

a) Parches de seguridad aplicables.
b) Procesos para monitorear, analizar y responder a alertas de seguridad.
c) Elementos adecuados de diseño de seguridad de red que proporcionen separación de datos.
d) Uso y actualización periódica de software antivirus.
e) Procesos para mantener, gestionar y proteger con regularidad el software instalado.
f) Los datos deben estar almacenados de forma segura en un centro de datos con la certificación ISO 27001 (o cualquier otra certificación ISO relevante) o SAS-70.
g) Cualquier infraestructura que aloje datos debe estar monitoreada para detectar ataques a la seguridad de la información a nivel de red, sistema operativo, base de datos y aplicación con el uso de sistemas de detección o prevención de intrusión.
h) El nivel adecuado de registros de auditoría a nivel de red, sistema operativo, base de datos y aplicación para detectar e investigar los ataques a la seguridad.
i) Las mejores prácticas de seguridad de la industria para brindar seguridad a nivel de red, sistema operativo, base de datos y aplicación web.

j) El proceso de gestión de correcciones para garantizar que todo el software esté actualizado con las correcciones de seguridad/versiones más recientes.
k) Procedimientos para responder a cualquier pregunta/llamada de Capgemini respecto a incidentes de seguridad en un lapso de veinticuatro (24) horas posteriores a la recepción del correo electrónico o llamada de Capgemini.
l) Elementos adecuados de diseño de seguridad de red que proporcionen separación de datos.
m) Uso y actualización periódica de software antivirus.

**13. DEBIDA DILIGENCIA/AUDITORÍAS.**

a) Capgemini se reserva el derecho a realizar una auditoría de seguridad si es necesario al menos una vez al año (para lo cual el Proveedor deberá asignar recursos pertinentes para permitir la auditoría de Capgemini), o el Proveedor proporcionará garantía continua respecto a la seguridad del negocio de Capgemini a través de la realización, al menos una vez al año, de una auditoría de seguridad por parte de un tercero independiente, así como evaluaciones periódicas de vulnerabilidad, pruebas de penetración y auditorías internas.
b) Los resultados de las auditorías y los planes para resolver los resultados de las auditorías deberán compartirse con Capgemini dentro de los treinta (30) días siguientes a que el Proveedor reciba los resultados de dichas auditorías. Además, el Proveedor debe reparar los hallazgos que tengan el potencial de afectar el negocio de Capgemini dentro de periodos mutuamente acordados.
c) La auditoría debe verificar como mínimo una evaluación de seguridad basada en normas internacionalmente reconocidas (ISO 27001, OWASP top 10, Matriz de control de CSA, según corresponda).
d) Capgemini podrá solicitar que se realice, a su propio costo, una prueba de penetración en la aplicación del negocio de Capgemini, lo cual no se realizará más de una (1) vez al año. Capgemini deberá notificar al Proveedor con antelación sobre cualquier prueba mediante la presentación de una solicitud al Proveedor y la formalización de un acuerdo de pruebas de penetración. El Proveedor y Capgemini acordarán un momento mutuamente aceptable para la prueba, lo cual por lo general será de treinta (30) días posteriores a dicha solicitud. Capgemini tendrá derecho de notificar al Proveedor en caso de que Capgemini detecte alguna vulnerabilidad. Tras dicha notificación, el Proveedor realizará de inmediato cualquier cambio necesario para proteger el negocio de Capgemini.

**14. RECUPERACIÓN ANTE DESASTRES.**

a) El Proveedor deberá tener implementados planes adecuados de continuidad de negocios y recuperación ante desastres basados como mínimo en los lineamientos de buenas prácticas del Instituto de Continuidad de Negocios (“BCI”). Dichos planes deberán ser aprobados por la administración sénior del Proveedor al nivel equivalente de un Director General (CEO) o Director de Operaciones (COO).
b) El Proveedor deberá recuperar todos los datos y brindar acceso al negocio de Capgemini dentro del objetivo de tiempo de recuperación (“RTO”) acordado.
c) El Proveedor deberá garantizar la recuperación de los datos hasta el objetivo de punto de recuperación (“RPO”) acordado.

d) El Proveedor deberá llevar a cabo pruebas de Recuperación ante Desastres como mínimo una vez al año. Los planes de pruebas deberán ponerse a disposición de Capgemini a solicitud.

**15. NOTIFICACIÓN Y MITIGACIÓN DE VULNERACIÓN DE SEGURIDAD.**

e) El Proveedor debe reportar a Capgemini cualquier vulneración de seguridad por escrito sin retraso injustificado después de hacerse de su conocimiento esta situación y dentro de un plazo máximo de veinticuatro (24) horas. Además, el Proveedor deberá proporcionar cualquier información adicional razonablemente solicitada por Capgemini para fines de investigar la vulneración de seguridad, así como cualquier otra información disponible que Capgemini requiera incluir para la persona de conformidad con las leyes al momento de la notificación o con prontitud después de la misma, ya que se retrasa la información.

a) En caso de alguna vulneración de seguridad, el Proveedor deberá subsanar a la brevedad dicha vulneración de seguridad y mitigar cualquier efecto dañino surgido de la misma. Del mismo modo, si, debido a alguna vulneración de seguridad, la legislación aplicable obliga a Capgemini a notificar a las personas afectadas, el Proveedor deberá reembolsar a Capgemini los costos razonables asociados a dichas notificaciones o, a elección del Proveedor, proporcionar la notificación directamente.