Requisitos de Seguridad de la Información para servicios de computación en la nube (SaaS, IaaS, PaaS), servicios web (web services) y servicios de hosting o alojamiento de información en internet

Metro de Medellín Ltda. reconoce que la información constituye un activo estratégico fundamental para la organización, clave en la generación y aumento de valor. En este sentido, se exige que los servicios contratados a terceros se presten dentro de un entorno controlado que permita mitigar los riesgos inherentes al uso de servicios de computación en la nube, servicios web y almacenamiento o alojamiento de información en internet, garantizando el cumplimiento de las siguientes características mínimas de seguridad:

Localización de los datos

El proveedor debe informar, desde la etapa precontractual y durante el contrato, el nombre del proveedor o centro de datos y la ubicación de los datos durante todo su ciclo de vida. Esto permite a LA EMPRESA evaluar riesgos y requisitos legales. Cualquier cambio de localización debe ser analizado y aprobado por LA EMPRESA.

1. **Centro de Datos.**

La aplicación o servicio debe estar alojada en un centro de datos de alta disponibilidad, en este caso debe ser con un proveedor de computación en nube que cumpla altos estándares de fiabilidad, escalabilidad y seguridad. El proveedor de nube en el cual se encuentre alojada la información de LA EMPRESA o que sea responsable de soportar el funcionamiento de la aplicación SaaS, debe cumplir como mínimo con las certificaciones en seguridad de la información ISO 27001:2013, SOC 1, SOC 2, SOC 3. En caso de que el servicio o aplicación se requiera para transmitir, procesar o almacenar información de tarjetas de pago deberá cumplir también con el estándar PCI DSS como mínimo la versión 3.2.1.

2. **Transferencia y Transmisión de Datos Personales**

En caso de realizar transferencia o transmisión de datos personales responsabilidad de LA EMPRESA a servicios o aplicaciones alojadas en infraestructura proporcionada por terceros, se debe cumplir con los establecido en la ley 1581 de 2012 y los demás lineamientos que la Superintendencia de Industria y Comercio ha dictado para tal fin:

“La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

La transmisión de datos personales por su parte implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia y tiene por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable."[1]

En Colombia, el artículo 26 de la Ley 1581 de 2012 regula la transferencia internacional de datos personales y prohíbe transferir datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos, salvo las excepciones que expresamente señala.

De acuerdo con lo establecido en el numeral 3.2 de la circular externa 002 del 23 de marzo de 2018 emitida por la Superintendencia de Industria y Comercio, los países que cuentan con un nivel adecuado de protección de datos personales son:

Alemania, Australia, Bélgica, Bulgaria, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, México, Noruega, Países Bajos, Perú, Polonia, Portugal, Reino Unido, República Checa, República de Corea, Rumania, Serbia, Suecia y los países que han sido declarados con el nivel adecuado de protección por la Comisión Europea.[2]

En caso de que se requiera transferir o transmitir datos a un destino que no se encuentre en la lista anterior, el responsable de tratamiento de datos personales deberá verificar si ese país cumple con las estándares fijados en el numeral 3.1 de la circular mencionada, verificar si cumple con una de las excepciones contempladas en el artículo 26 de la ley 1581 de 2012, obtener la aprobación expresa por parte de los titulares de los datos personales u obtener una declaración de conformidad emitida por la Superintendencia de Industria y Comercio.

3. Independencia de la Información

El proveedor debe garantizar la independencia y seguridad de la información almacenada por LA EMPRESA, es decir, que la instancia de la aplicación deberá ser exclusiva para LA EMPRESA.

El proveedor debe suministrar a LA EMPRESA el diagrama que describa la arquitectura del servicio ofertado.

4. Desarrollo Seguro de la Aplicación o Servicio

[1] http://www.sic.gov.co/preguntas-frecuentes-pdp
[2] http://www.sic.gov.co/sites/default/files/normatividad/032018/CIRCULAR-EXTERNA-002.pdf

EL proveedor debe informar si para el servicio o aplicación ofrecida y sus componentes, utiliza metodologías o buenas prácticas para el desarrollo seguro de software. A continuación, algunas de las más utilizadas:

- Proyecto abierto de seguridad de aplicaciones web (OWASP, por sus siglas en inglés)
- Ciclo de vida de desarrollo de seguridad de Microsoft (Microsoft SDL, por sus siglas en inglés).
- Modelo de Madurez para Aseguramiento de Software (SAMM, por sus siglas en inglés).

5. Seguridad en aplicativos de software como servicio (SaaS):

El proveedor debe garantizar la seguridad del aplicativo y la infraestructura de hardware y software que lo soporta, cumpliendo como mínimo con las mejores prácticas descritas en ISO27001:2013 en cuanto al manejo de usuarios, contraseñas, puertos abiertos, servicios habilitados, separación de ambientes, definición de permisos, versiones actualizadas, (endurecimientos de hardware y software).

El proveedor deberá tener implementados controles técnicos de seguridad de la información, por ejemplo, un cortafuegos para aplicaciones web (WAF, por sus siglas en inglés), que reduzcan la posibilidad de que se exploten vulnerabilidades críticas como las mencionadas en el top 10 del Open Web Application Security Project (OWASP).[3]

El proveedor deberá describir y entregar evidencia de los controles con los que cuenta.

6. Navegación segura

La aplicación o servicio web debe soportar el acceso a través de navegación segura, es decir, deberá contar con certificado digital https con validación extendida emitido por una entidad certificadora reconocida. El proveedor debe suministrarlo y configurarlo en la solución. Es responsabilidad del proveedor asignar y suministrar el direccionamiento público requerido para la URL a la cual accederán los usuarios de la plataforma. La solución deberá soportar la configuración e instalación de certificados digitales suministrados por LA EMPRESA en caso de requerir que sea accedida de manera segura a través de un dominio o subdominio propiedad de LA EMPRESA.

7. Intercambio seguro de información

La solución debe soportar el cifrado de los datos en el tránsito. En caso de requerirse la integración de esta con otros sistemas de información de LA EMPRESA, será establecida a través de la creación de una red privada virtual (VPN, por sus siglas en inglés) sitio a sitio entre el servicio o aplicación web del proveedor y LA EMPRESA.

[3] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

El proveedor debe hacerse cargo del suministro y configuración del cliente VPN IPsec de tipo site-to-site que sea compatible con el firewall de la Empresa y una IP pública a la cual se le puedan configurar las reglas de acceso.

En caso de ser requerido, el proveedor deberá suministrar a LA EMPRESA los datos de direccionamiento IP privado y público que sean necesarios para establecer reglas en los dispositivos de seguridad que permitan el intercambio seguro de información entre las partes.

8. Políticas de Seguridad Informática

EL proveedor seleccionado, al inicio del contrato, deberá suministrar a LA EMPRESA un documento que describa las políticas de seguridad de la información implementadas al interior de su empresa y deberá certificar que los empleados que harán parte de la ejecución del contrato cuentan con el conocimiento y apropiación de estas.

9. Reporte y atención de Incidentes de Seguridad Informática

EL proveedor seleccionado, al inicio del contrato, debe enviar a LA EMPRESA un documento que describa los procedimientos que tiene establecidos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes de seguridad informática. Igualmente, deberá certificar que tiene identificados y realiza una adecuada evaluación, tratamiento, control y seguimiento de los riesgos informáticos asociados al servicio contratado. En dicho procedimiento deberán estar claramente establecidos los tiempos que aplican para la investigación de los incidentes y su reporte a las partes interesadas.

Para la gestión e investigación de los incidentes de seguridad, el proveedor deberá garantizar el cumplimiento de los requisitos legales aplicables.

EL OFERENTE deberá reportar a LA EMPRESA los eventos o incidentes de seguridad que afecten o tengan el potencial de afectar la prestación del servicio contratado, la información intercambiada entre las partes, los sistemas de información de LA EMPRESA o la información alojada en estos, y todas aquellas situaciones de alto riesgo que sean detectadas por los sistemas de monitoreo y control o en auditorías que realiza el proveedor con sus recursos. De la misma forma deberá informar a LA EMPRESA los planes de remediación aplicados o por aplicar.

10. Auditorías de seguridad.

Antes de la puesta en producción y por lo menos cada seis (6) meses el proveedor, con sus propias herramientas o través de un tercero autorizado, deberá realizar auditorías técnicas de seguridad sobre el aplicativo o servicio web y la infraestructura que lo soporta con el fin de identificar posibles vulnerabilidades técnicas que pongan en riesgo la información de LA EMPRESA y la disponibilidad del servicio. Entre las pruebas requeridas se resaltan las pruebas de penetración (Pentesting) o hacking ético y escaneo de vulnerabilidades sobre aplicaciones web (web application scan). El informe de las auditorías de seguridad realizadas y las remediaciones aplicadas deberán ser entregados a LA EMPRESA.

En caso de que LA EMPRESA lo requiera podrá realizar sus propias auditorías técnicas sobre el servicio contratado, con la previa aprobación del proveedor y con la coordinación y planificación de ambas partes, sin que esto implique sobre costos, ni afectación del servicio. El resultado del análisis de vulnerabilidades será compartido con el proveedor para que este realice la remediación de las vulnerabilidades encontradas en un plazo acordado entre las partes.

11. Garantía sobre el tratamiento de la información de LA EMPRESA.

Toda la información y/o documentación relativa a LA EMPRESA que sea intercambiada entre las partes para la ejecución del contrato, así como la información transitada y almacenada en el aplicativo o servicio web, debe efectuarse con la finalidad exclusiva de la prestación de los servicios objeto del presente contrato y se debe realizar bajo el deber general de confidencialidad y secreto. EL proveedor asume el compromiso expreso de no utilizar la información y/o documentación suministrada para cualquier propósito distinto que no sea la prestación de los servicios contratados por LA EMPRESA.

Esta condición debe ser extensiva para los empleados del proveedor y están obligados, no sólo al secreto profesional absoluto, sino también a la neutralidad y máxima discreción frente a otros clientes o interesados en la solución.

12. Entrega de los datos almacenados y destrucción de la información almacenada

En caso de finalización del contrato por vencimiento del tiempo contratado u otros motivos, el proveedor deberá entregar un archivo que contenga toda la información de LA EMPRESA y sus colaboradores que se encuentre almacenada en las bases de datos de la aplicación o servicio contratado. El formato del archivo entregado será definido entre las partes con el fin de que la información que contenga sea completamente accesible por LA EMPRESA sin depender del proveedor. El plazo máximo para la entrega de la información a LA EMPRESA es de diez (10) días calendario una vez solicitada.

Una vez finalizada la relación comercial la información de LA EMPRESA y sus colaboradores que se encuentre almacenada en las bases de datos de la aplicación o servicio contratado debe ser destruida con procedimientos que garanticen la no recuperación de esta. El proveedor una vez realizado el borrado seguro de la información y en un plazo máximo de quince (15) días calendario contados a partir de la fecha fin del servicio contratado, deberá suministrar una certificación firmada por el representante legal en la que brinde información sobre el procedimiento aplicado, así como las herramientas de hardware y software, técnicas o algoritmos utilizados para el borrador de la información.

En caso de que LA EMPRESA desee dar continuidad al servicio le informará al proveedor para que suspenda el procedimiento de borrado seguro de la información

13. Logs del servicio

La solución debe mantener un registro de actividades de usuario fácilmente accesible para LA EMPRESA, con el fin de examinar las actividades realizadas por cada usuario de la aplicación. Debe permitir parametrizar que el único usuario autorizado para acceder al log o registro de actividades sea el usuario Administrador u otro indicado por LA EMPRESA.

El periodo de retención de los logs debe ser mínimo de 30 días calendario.

14. Acuerdos de Nivel de Servicio (ANS) y Métricas del servicio

La aplicación o servicio web debe tener una disponibilidad mínima del 99,9% al año, equivalente a 43156.8 minutos/mes con respecto a una disponibilidad esperada de 24/7. La disponibilidad de infraestructura no incluye las paradas planificadas. Los tiempos de indisponibilidad del servicio por actualización de la plataforma que requiera paradas planificadas o trabajos programados serán estipulados para cada actuación entre las partes.

El proveedor debe contar con las herramientas que permitan medir el cumplimiento de estas métricas.

15. Recuperación ante desastres

El proveedor debe garantizar la recuperación y continuidad del servicio ante problemas físicos o lógicos en un tiempo máximo de 1 hora, sin pérdidas de información para LA EMPRESA.

16. Protección de datos personales

El proveedor y su servicio se encontrarán obligados al cumplimiento de la ley estatutaria 1581 de 2012 y el Decreto 1377 del 27 de junio de 2013.