Versión: 1.0 de octubre 28 de 2016

TÉRMINOS DE PROCESAMIENTO DE DATOS PARA LA SOLUCIÓN INTERNA

1. Introducción:

Con estas disposiciones, Gemalto desea informar al cliente del procesamiento de datos, lo que incluye los Datos Personales (como se definen abajo) a los que Gemalto puede tener acceso al proporcionar al cliente el Servicio de Asistencia (como se define abajo) que cubre la Solución Interna (como se define abajo).

2. Algunas definiciones

Según se utilizan en el presente documento,

Componentes de Back-End significa que cualquier componente que se ejecute en las instalaciones del cliente donde está instalada la Solución Interna se considera como un componente de back-end en el contexto de estos términos de procesamiento de datos. Esto incluye a los servidores de aplicaciones, los servidores de bases de datos, los componentes de infraestructura subyacente como serían los routers, cortafuegos, así como cortafuegos de aplicaciones web si forman parte de lo entregado por Gemalto al Cliente

Información del Cliente es la información personal que Gemalto puede recopilar a partir de las interacciones de los empleados o agentes del cliente con Gemalto en la prestación de los Servicios de Asistencia.

Ley de Protección de Datos Personales se refiere a todas las leyes, reglas, regulaciones, requisitos gubernamentales, códigos y leyes internacionales, federales, estatales y provinciales aplicables a los datos de carácter personal.

Solución interna es la solución de Gemalto para la cual se concede una licencia al cliente, que está instalada en las instalaciones del cliente y que éste gestiona.

Sistema de gestión es la plataforma basada en la web de emisión de tickets conocida como STiM y que Gemalto utiliza en relación con el suministro del Servicio de Asistencia.

Datos personales son (i) los datos que se refieren a un individuo viviente (ya sea en su vida personal o familiar, negocio o profesión) que puede ser identificado (a) a partir de esos datos, o (b) a partir de los datos y otra información que estén en posesión del controlador de los datos, o que puedan llegar a su posesión, así como (ii) información que puede utilizarse para identificar o rastrear la identidad de una persona, lo que incluye, entre otros datos, su nombre, dirección, número de la seguridad social, datos biométricos, fecha de nacimiento, etc.

Apoyo remoto es el uso del teléfono, correo electrónico o una VPN para facilitar la resolución de una solicitud.

Solicitud es una petición de un cliente relacionada con el suministro del Servicio de Asistencia.

Registro de solicitudes es un registro en el sistema de gestión generado por Gemalto que anota las solicitudes y les da seguimiento.

Datos de servicio son los datos que residen en la Solución Interna a los que se da acceso a Gemalto a fin de realizar los Servicios de Asistencia.

Departamento de Servicio es el grupo de asistencia técnica de Gemalto que actúa como punto de contacto único entre Gemalto y el cliente a fin de administrar todas las solicitudes, comunicaciones y remisiones a instancias superiores con el Cliente.

Servicio de Asistencia es el objeto del servicio de asistencia de un acuerdo de nivel de servicio convenido.

VPN es una red privada virtual y proporciona un mecanismo de comunicación seguro para datos y otra información que se transmite entre dos puntos finales.

3- **Procesamiento de la Información del Cliente**

En el momento de una solicitud, Gemalto está recolectando Información del Cliente que está almacenada en el sistema de gestión ubicado en Francia. El objetivo de tal recolección es identificar el origen de la Solicitud, asociar ésta con el Cliente, a fin de analizar, diagnosticar y resolver la Solicitud, y para efectos de facturación, mejoras de la Solución Interna y seguridad.

La Información del Cliente se puede transferir al equipo de asistencia que suministra el Servicio de Asistencia, siempre que dicho equipo provoque una transferencia transfronteriza de datos sujeto a los términos de la sección 6 que aparece abajo.

4- **Apoyo remoto**

El Servicio de Asistencia se proporciona a través de un Departamento de Servicio (Nivel 1 de asistencia) ubicado en India, en SAFENET INFOTECH PVT LTD (una entidad legal miembro del grupo empresarial Gemalto). El Departamento de Servicio crea un registro de solicitud en el Sistema de Gestión y coordina la respuesta según el acuerdo de nivel de servicio convenido.

Si la solicitud tiene que ser remitida al Nivel 2 de asistencia, los expertos a cargo de dicho nivel se encuentran localizados según lo especificado por Gemalto en la oferta contractual/comercial según el caso.

Si Gemalto tiene la opinión de que una Solicitud requiere una conexión remota a la Solución Interna, se conectará a ésta a través de una VPN segura instalada previamente con el Cliente.

El Cliente debe proporcionar a Gemalto acceso a la Solución Interna donde y cuando lo necesite en relación con una Solicitud.

La conexión remota a la Solución Interna está cubierta por los términos de seguridad estipulados en la Sección 5.

Si el Cliente tiene una política de seguridad o un proceso de asistencia a los que espere que se ajuste Gemalto, éste se reserva el derecho de revisar la política o el proceso y:

a) confirma que puede cumplirlos (sujeto a cargos adicionales); o bien

b) si no es capaz de cumplirlo, Gemalto no tendrá obligación de adherirse a la política o el proceso.

Cuando esté conectado remotamente a la Solución Interna, Gemalto tiene la capacidad de ver y usar los Datos de Servicio con el único propósito de proporcionar el Servicio de Asistencia. Gemalto no copia, modifica ni elimina los datos de servicio.

5- **Términos de seguridad**

5.1El Servicio de Asistencia sigue estos principios de seguridad:

- solamente se autoriza a las personas que necesitan acceso remoto;
- sólo se pueden realizar acciones autorizadas;
- el acceso a la Solución Interna se realiza a través de una interfaz confiable;
- se monitorizan las actividades sospechosas;

- se hace el seguimiento de las acciones para identificar roles y responsabilidades en caso de que haya investigaciones.

Más exactamente:

5.1.1 Aislamiento

Para aislar la Solución Interna a la infraestructura de Gemalto, éste propone dos soluciones:

a) La primera se basa en un servidor de salto, que bloquea los accesos directos de los operadores de los PC a la Solución Interna. Las operaciones sólo se pueden realizar desde el servidor de salto. Dado que el operador no tiene el derecho de administración de este servidor de salto, sólo puede utilizar software autorizado ya instalado en el servidor de salto;

b) La segunda solución se basa en una infraestructura dedicada. El operador tiene una PC dedicada sobre la cual dispone de derechos limitados. Hay software específico preinstalado en este equipo para realizar el mantenimiento y las operaciones de asistencia. Hay un servidor de archivos disponible para la transferencia de archivos de bitácora. También hay un antivirus instalado en este PC dedicado a fin de evitar cualquier infección.

El objetivo de estas dos soluciones es limitar tanto como sea posible el uso de aplicaciones inadecuadas y la transferencia de archivos no deseados entre la Solución Interna y las instalaciones de Gemalto.

El segundo aspecto de este aislamiento se relaciona con el portador entre las infraestructuras. El canal de comunicación también tiene que protegerse. Para ambas soluciones, es obligatorio el uso de una VPN a fin de proteger el vínculo entre la Solución Interna y las instalaciones de Gemalto.

5.1.2 Autenticación

El segundo aspecto importante es la capacidad de autenticar al operador. Esta autenticación debe ser lo suficientemente fuerte como para evitar una usurpación de identidades y para ser inaplicable en el caso de procedimientos legales.

Gemalto ha implementado su propio sistema basado en su sistema de autenticación de dos factores de forma. Se concede el acceso a la PC dedicada o al servidor de salto con la insignia personal del empleado. Esta insignia es única e incrusta una clave privada que se utiliza para esta autenticación.

Para tener acceso a estos sistemas, el operador debe presentar su insignia y el PIN asociado. La insignia combinada con un LDAP (Lightweight Directory Access Protocol) central proporciona varias ventajas. La primera de ellas consiste en validar la insignia en sí misma. La segunda es permitir una gestión de grupo. Con base en la autenticación LDAP, el sistema valida los accesos de los derechos del operador al servidor de salto y a la Solución Interna. El último punto es la facilidad de la gestión de accesos. La gestión de accesos y revocaciones de los recién llegados en el sistema central. Gracias a este método de autenticación fuerte, Gemalto garantiza que sólo las personas que se requiera tengan acceso a la Solución Interna. Más aún, basándose en las definiciones de roles y de grupos, los derechos de acceso se limitan a la prestación del Servicio de Asistencia.

5.1.3 Auditabilidad

Además, con esta autenticación fuerte, se hace factible la capacidad de conseguir una detección de comportamientos sospechosos en tiempo real o realizar más análisis en caso de incidentes.

La detección en tiempo real se basa en detectores de seguridad a cargo del envío de alertas de seguridad. Estas alertas disparan un proceso interno a cargo de definir la importancia de la detección y para poner en marcha las acciones de contención correspondientes.

Los sistemas de bitácora registran las acciones realizadas por los operadores. Gracias al sistema de autenticación fuerte, las bitácoras asocian al dueño y a las acciones.

Debido a la confidencialidad de ciertos datos, las bitácoras están higienizadas. Estas bitácoras se almacenan en un espacio seguro y sólo los oficiales de seguridad pueden tener acceso a ellas.

Estos sistemas combinados permiten que Gemalto detecte los casos de alertas de seguridad y reaccione a ellos.

5.2 Confirmación del Cliente

El Cliente confirma y entiende que todos los componentes de back-end de la Solución Interna que ofrece Gemalto tienen por objeto ejecutarse en un entorno seguro y controlado. Se espera que tal entorno seguro y controlado esté alineado con las mejores prácticas que se aplican en cada área, desde la seguridad física a la lógica. Gemalto ha elegido la norma ISO27002 como catálogo adecuado de mejores prácticas de seguridad. Las características de seguridad específicas de la Solución Interna las pone a disposición Gemalto a petición. El Cliente acepta asumir todas las responsabilidades por no implementar las características de seguridad anteriormente mencionadas o no solicitar las características de seguridad específicas de la Solución Interna.

6- **Transferencia transfronteriza**

6.1 Como se indica en la Sección 4 anterior, la prestación del Servicio de Asistencia puede crear una transferencia transfronteriza de la información o datos de asistencia del Cliente; el cliente entiende que tal traslado transfronterizo de su información o datos de asistencia puede estar sujeto a requisitos específicos impuestos por la ley de protección de datos personales aplicable donde la carga de tales requisitos específicos la tiene el cliente al ser la entidad que pone a disposición de Gemalto la información o Datos de Asistencia del Cliente.

6.2 En caso de que tal traslado transfronterizo de la información o Datos de Asistencia del Cliente pudiera requerir la celebración de un acuerdo específico de transferencia transfronteriza a la luz de la ley de protección de datos personales aplicable. Gemalto y el Cliente colaborarán con el fin de cumplir con este requisito.
