

Relación con proveedores

ITAPP

Contenido

1. Antecedentes, listado de proveedores y servicios ITAPP	2
2. Requisitos de seguridad en productos y servicios	3
3. Documentación del acuerdo.....	5
4. Ciclo de vida para la gestión de la relación con los proveedores	5

1. Antecedentes, listado de proveedores y servicios ITAPP

- **Google**
 - Proveedor de servicio tecnológico
 - Máquinas virtuales
 - Dominio
 - Servicios de soporte informático
 - Datos a los que tiene acceso:
 - Configuraciones
 - Tecnologías en uso
 - Medidas de seguridad
 - Estructura del producto Itapp
- **Amazon**
 - Proveedor de servicio tecnológico
 - Máquinas virtuales
 - Servicios de soporte informático
- **Apache**
 - Suministrador de producto tecnológico
 - Apache Spark
 - Apache Hadoop
 - Apache Kafka
 - Apache Nifi
- **Gitlab**
 - Proveedor de servicio tecnológico
 - Repositorio
- **Twitter Tumblr**
 - Datos

2. Requisitos de seguridad en productos y servicios

- En términos de control de acceso, determinar qué información es accedida, cómo puede ser accedida y la clasificación y protección de esta.
 - Los proveedores de servicios tecnológicos son los encargados de gestionar las credenciales de acceso para dichos servicios de las cuentas de Itapp.
Si la gestión de dichas credenciales no es llevada de forma correcta se compromete el acceso, y, por lo tanto, la confidencialidad de cualquier dato asociado.
 - Cualquier tipo de credencial o dato proporcionado a un proveedor de servicio que se vaya a guardar ha de ser codificado para asegurar la confidencialidad tanto en tránsito, como en el guardado como en una migración.
- Asegurarse de que, una vez finalizado el contrato, el proveedor ya no podrá acceder o mantener la información sensible de nuestra organización.
 - Cada dato asociado a una cuenta de un proveedor de servicio tecnológico deberá de ser borrado y mantenerse inaccesible para cualquier agente una vez finalice el contrato con Itapp.
 - Itapp se compromete a permitir la posesión de dichos datos en caso de que estos sean anonimizados de acuerdo con los Términos y Condiciones de Servicio del proveedor, si se especifica.
 - En caso de que algún proveedor fije en los Términos y Condiciones de Servicio un periodo post finalización de contrato donde los datos se mantengan guardados de cara a una posible renovación, esto se respetará, siempre y cuando se cumpla con los puntos anteriores.
- Metodología de finalización de contrato:
 - En caso de que existan, el proveedor de servicio o producto es el encargado de señalar cuales son los activos a ser devueltos por Itapp.
 - Cualquier credencial de inicio debe ser desactivado y borrado.
 - El borrado de información se atiene a los puntos expresados en el anterior requisito.
- Reflejar los requisitos legales oportunos:
 - Cumplimiento del RGPD
 - Cumplimiento de los derechos de propiedad intelectual
- Certificación de los servicios contratados:

- Itapp cumple con la certificación ISO 27001, de la misma manera, a cualquier proveedor se le exige cumplir con la misma certificación.
- Reflejar el derecho de auditoría y de control sobre aspectos relevantes del acuerdo.
 - El contratante de un servicio o producto tiene derecho a comprobar que la otra parte contratante está cumpliendo con lo estipulado. Del mismo modo Itapp se reserva el derecho de comprobar que el servicio o producto contratados cumplen con los requisitos reflejados en el checklist/contrato.
 - En caso de que no se cumplan los requisitos reflejados, Itapp se reserva el derecho a cerrar el contrato y tomar medidas punitivas.
 - Itapp se compromete a cumplir con las Políticas de Uso Adecuado y Condiciones y Directrices adicionales establecidas por los proveedores de cualquier producto o servicio.
 - Esto incluye:
 - Violar o impulsar la violación de los derechos legales de terceros.
 - Copyright
 - Tomar parte en o impulsar actividad ilegal.
 - Actividades difamatorias o de objetivos fraudulentos.
 - Interferir con la disponibilidad del servicio o producto para otros usuarios.
 - Cualquier otra condición o directriz especificada.
 - Itapp se compromete a facilitar información que ayude a verificar que Itapp está cumpliendo con lo establecido en los documentos anteriores en base a lo acordado en el contrato con los proveedores.
 - En el caso de que estos requisitos no se cumplan por alguna de las partes, cualquier parte tiene el derecho de finalizar el contrato.
- Penalizaciones por incumplimiento de garantías:
 - En caso de que el acceso a un servicio se bloquee por motivos erróneos o la confidencialidad de los datos se pierda se tomarán acciones legales punitivas en el extenso permitido por el marco legal.

3. Documentación del acuerdo

El checklist de requisitos de seguridad a cumplir se adjunta en un Excel junto a este documento. Dicho Excel será el utilizado para crear los contratos a firmar por los proveedores e Itapp y será sobre el cual se basen los chequeos de los requisitos durante el ciclo de vida para la gestión de la relación con los proveedores.

4. Ciclo de vida para la gestión de la relación con los proveedores

Cada contrato que Itapp acepta con un proveedor para el uso de un servicio o producto se comprobará contra el checklist de requisitos de seguridad. Esta comprobación se realizará por los responsables de datos de Itapp, sin embargo, en algunos casos, se hará compulsoria la asistencia de todos los miembros del equipo.

En caso de que el servicio contratado sea de pago periódico cuando se acerque el momento de renovar el contrato con un pago, se revisará si dicho proveedor cumple con los requisitos recogidos en el checklist en dicho momento. También se revisará si durante la contratación se ha dado algún evento que haya hecho cuestionar al personal de Itapp el continuar usando los servicios de ese proveedor (brechas de seguridad recientes, cambios en sus políticas de uso, niveles de servicio, etc.) aunque estos no hayan afectado negativamente a Itapp.

En caso de que alguno de los proveedores cambie sus Términos y Condiciones de Uso, Niveles de Servicio y/u otras condiciones que afecten a los servicios y productos usados por Itapp, se realizará la misma revisión.

En caso de que el servicio contratado sea gratuito y no haya una periodicidad de renovaciones contractuales, el personal de Itapp revisará en la finalización del calendario financiero de ese año el continuar o no utilizando los servicios de dicho proveedor.

En este último caso se pedirá la asistencia de todo el personal al chequeo del ciclo de vida, así consiguiendo que todos los trabajadores de Itapp estén familiarizados del porqué del uso de cada servicio, en qué condiciones se están usando y cada uno podrá aportar ideas y opiniones sobre por qué seguir usando o no un servicio y de si existe un servicio o producto mejor.

En resumen, las fechas clave para el ciclo de vida para la gestión de la relación con los proveedores son:

- Fechas previas a renovación de pagos.
- Finalización del calendario financiero.
 - Reunión obligatoria para todo el personal.
- Fechas donde se oficializan cambios en las condiciones contractuales de los proveedores.

NIVEL	ALCANCE	CONTROL	
B	PRO	Requisitos de seguridad en productos y servicios Estableces los requisitos de seguridad mínimos que deben cumplir los productos que adquieres y los servicios que contratas.	<input type="checkbox"/>
A	PRO	Definir cláusulas contractuales en materia de seguridad de la información Eres riguroso en la elaboración y aceptación de las cláusulas contractuales en materia de ciberseguridad.	<input type="checkbox"/>
B	PRO	Definir las responsabilidades concretas por ambas partes Delimitas las responsabilidades en materia de ciberseguridad para cada una de las partes involucradas.	<input type="checkbox"/>
B	PRO	Definir los ANS (Acuerdos de Nivel de Servicio) Defines en detalle los ANS a los que sometes los servicios contratados.	<input type="checkbox"/>
B	PRO	Controles de seguridad obligatorios Determinas que controles de seguridad son de obligado cumplimiento en las relaciones con tus proveedores de servicios tecnológicos.	<input type="checkbox"/>
B	PRO	Formar parte de los foros y organizaciones de usuarios de los productos/servicios software utilizados Participas en las organizaciones de usuarios de los productos y servicios software que adquieres. Controlas la reputación de tus proveedores.	<input type="checkbox"/>
B	PRO	Certificación de los servicios contratados Exiges a tus proveedores certificaciones que garanticen la calidad en materia de seguridad de ciertos servicios contratados de especial criticidad.	<input type="checkbox"/>

NIVEL	ALCANCE	CONTROL	
B	PRO	Auditoría y control de los servicios contratados Supervisas que los productos y servicios contratados responden a lo acordado en materia de ciberseguridad.	<input type="checkbox"/>
B	PRO	Finalización de la relación contractual Garantizas la seguridad de tu información tras la finalización de un servicio o contrato.	<input type="checkbox"/>

Revisado por: _____

Fecha: _____