Objetivo

Describir los lineamientos que ASIC debe adoptar para asegurar la protección de los activos de la organización que sean accesibles a los proveedores, así como mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

Política de Seguridad con Proveedores

En las situaciones en que se requiera contratar servicios de tratamiento o resguardo de activos de información, tales como servicios de hosting e infraestructura, plataforma tecnológica, centros de datos y procesamiento, almacenaje de información física o digital, entre otros, se deberá verificar que el proveedor cuenta con mecanismos y controles de seguridad adecuados, los que deberán tener, al menos, el mismo estándar de seguridad que el implementado en ASIC S.A.S.

Asimismo, en estas situaciones, se deberá realizar una evaluación de riesgos de seguridad asociados al servicio entregado por el proveedor, con la finalidad de identificar brechas que puedan ser potenciales vulnerabilidades que expongan la continuidad operativa de los procesos o puedan dañar la imagen Institucional, para lo cual el área requirente en conjunto con el líder de Seguridad de la Información, deberán realizar este análisis previo a la contratación del servicio o adquisición del producto.

Por su parte, para el caso en que existan proveedores que desarrollen sistemas de información para la Institución, se deberá considerar la revisión de los productos elaborados a partir de revisiones técnicas por parte del área de Tecnología de la información (TI).

Finalmente, en caso que los sistemas de información sean expuestos a la red de Internet, se deberá considerar además la ejecución de pruebas de seguridad que permitan garantizar razonablemente la confidencialidad, integridad y disponibilidad de los datos manipulados en el sistema.

El líder de seguridad de la información será el encargado asesorar la realización del contrato de que se trate, con el objeto de que puedan evaluarse adecuadamente los riesgos implicados que tengan relación con la seguridad de la información, así como la implementación de medidas de seguridad para mitigarlos y que de esta manera se puedan incluir los acuerdos requeridos para el cumplimiento en materia de confidencialidad, integridad y disponibilidad de la información a la que se tenga alcance.

En cada ocasión en que un proveedor requiera información de ASIC S.A.S. o cualquiera de sus clientes, que sea adicional a aquella que el Servicio se ha obligado a entregar en virtud

del contrato respectivo, o que no sea inherente a la naturaleza del mismo, el propietario de la información analizará los motivos de dicho requerimiento y procederá a aprobar o rechazar la entrega de la misma.

El acceso físico por parte de los proveedores a los activos de información deberá ser controlado y supervisado por personal administrativo o técnico, según sea el caso.

En las áreas protegidas o de alto riesgo, como centros de datos, se deberán establecer procedimientos documentados formales que tengan por objeto gestionar la forma en que se realizarán los trabajos en su interior, el que deberá contar con medidas de registro de proveedores, como también controles detectivos y preventivos.

Los proveedores podrán acceder en forma remota a los activos tecnológicos a través de herramientas de acceso remoto con supervisión visual total del responsable del activo en el área de TI, o a través de conexión VPN cuando ello fuere necesario para el cumplimiento de las obligaciones que emanan del contrato respectivo. Para la creación de accesos VPN, ASIC S.A.S., deberá implementar controles que permitan limitar accesos y registrar acciones para seguimiento. Los accesos VPN deberán estar controlados y restringidos a casos específicos en los que sea de obligatorio uso para el cumplimiento de las funciones y las solicitudes deberán ser validadas en conjunto por el propietario de la información y el líder de seguridad de la información, quienes analizarán los motivos de dicho requerimiento y procederán a otorgarla o denegarla.

En cualquier caso, dicho acceso será gestionado por el área de TI y sólo podrá tener por finalidad dar soporte a equipos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de seguridad y/o monitoreo.

Deberá existir un registro de los accesos que se han realizado a través de las herramientas aprobadas por el área de TI para efectos de trazabilidad y posterior revisión en caso de ser requerido.

Cuando se requiera elaborar un contrato particular con proveedores que tenga relación con servicios de tratamiento, manipulación, transmisión o almacenamiento de activos de información, ya sea en formato físico o digital, se deberán incorporar cláusulas de seguridad que permitan garantizar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, tales como acuerdos de niveles de servicios (SLA), derechos de auditar los procesos involucrados, los procedimientos aplicados frente a incidentes de seguridad, cláusulas de confidencialidad y no divulgación de información, como también la extensión de dichos deberes a empresas subcontratadas.

Para efectos de velar por la aplicación de cláusulas de seguridad en los contratos, bases de licitación, tratos directos, actos administrativos o cualquier otro documento formal relacionado a la contratación de servicios de proveedores, será responsabilidad del área jurídica, aplicar las modificaciones respectivas a los documentos administrados y elaborados al interior de la compañía con respecto a dicha materia.

En situaciones en que proveedores requieran hacer instalaciones de activos de información de carácter tecnológico, tales como servidores, equipos de red, equipos de soporte, entre otros, será requisito base implementar configuraciones que cumplan con el estándar de seguridad establecido por ASIC S.A.S., para lo cual, en caso necesario, deberán considerar ajustes en el acceso a los equipos, el monitoreo de capacidad, la sincronización de hora, el registros de auditoría y los servicios de nombre de dominio.

El área de TI tendrá la responsabilidad de verificar y validar la configuración de los equipos instalados, así como también de reportar las debilidades y oportunidades de mejora al proveedor del servicio a través de los procedimientos internos establecidos para estos efectos.

Para asegurar que los proveedores que prestan servicios en el tratamiento de información de propiedad de la compañía o sus clientes cuenten con estándares y niveles adecuados en materia de seguridad, ASIC S.A.S. se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas a riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los que para cualquier efecto serán facilitados de manera temporal y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.

Adicionalmente, la compañía también podrá realizar visitas programadas y supervisadas a las instalaciones de los proveedores, específicamente aquellos que presten servicios de resguardo de activos de información, esto con el objeto de verificar en terreno las condiciones de seguridad implementadas, todo esto coordinado a través del área de TI y el proveedor respectivo.

En los casos en que se requiera entregar información a proveedores, o que producto de la prestación del servicio acceda a información de la compañía, se deberán aplicar acuerdos de confidencialidad y no divulgación entre ASIC S.A.S. y los proveedores, los que deberán dar cuenta de los responsables, la información en cuestión, las medidas mínimas de seguridad aplicadas, la forma de proceder frente a incidentes, la extensión del acuerdo a terceros subcontratados, la propiedad de los productos desarrollados, el tiempo de vigencia del acuerdo, las sanciones frente a su incumplimiento y su aceptación formal.

La aplicación de los acuerdos de confidencialidad será responsabilidad de cada área requirente, sin embargo, su redacción estandarizada y el resguardado de los acuerdos ya formalizados será responsabilidad del área jurídica de la compañía.

En todo intercambio de información entre ASIC S.A.S. y los proveedores de servicios o productos, se deberán implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar razonablemente la seguridad en el acceso y la transferencia de información, considerando la aplicación de cifrado en las comunicaciones y la validación de identidad.

Para los casos en que existan proveedores que requieran acceder a información confidencial o interna, se deberá hacer entrega en medios que consideren criptografía basada en herramientas con cifrado robusto, para lo cual el área de TI y Soporte asesorará a los funcionarios de la mejor forma posible en esta materia.

De preferencia los proveedores que entreguen sus servicios a la compañía, sea cual fuere la modalidad de contratación utilizada, deberán contar con certificaciones vigentes relativas a la seguridad de la información aplicado a los procesos de servicios que deseen contratarse y sobre todo en los casos en que se externalice los procesos de tratamiento y resguardo de información, ya sean hosting, housing, entre otros. Dichas certificaciones podrán contemplarse además como requerimientos y/o factores de evaluación en los procesos de licitación, así como también a los procesos internos para la adopción e incorporación de mejores prácticas aplicadas los procesos de compra.

Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean entregados a la compañía en modalidad de servicio, también conocidos como servicios en la nube, además de los equipos tecnológicos que sean adquiridos o sistemas de información que sean desarrollados por terceros y sobre los cuales existan garantías del fabricante, se deberán establecer y documentar procedimientos para la gestión de incidentes de seguridad, los que serán gestionados a través de la mesa de servicios bajo los procedimientos internos ya definidos.

Los procedimientos para la gestión de incidentes que estén relacionados con proveedores, en los términos referidos en el párrafo anterior, deberán ser comunicados y formalizados entre las partes. Asimismo, ASIC S.A.S., podrá solicitar informes relacionados con las mediciones de incidentes de algún período, información que deberá estar disponible durante lo que dure la relación con el proveedor. El procedimiento de seguridad para la gestión de incidentes en cada caso deberá señalar, al menos, la persona de contacto, así como el número telefónico y/o correo electrónico al cual habrá que dirigir las solicitudes.

De los acuerdos de niveles de servicios y los planes de recuperación, la compañía considera relevante mantener la disponibilidad permanente de los servicios entregados por los proveedores, para lo cual se deberán establecer acuerdos de niveles de servicio que permitan garantizar razonablemente este principio, los que deberán ser formalizados, siendo estos medidos y monitoreados permanentemente.

Para el caso de los servicios relacionados con Tecnología, se considerarán como criterios relevantes relacionados con el nivel de servicio la entrega continua del mismo, los tiempos de respuesta de atención para su entrega, los tiempos de resolución de problemas, entre otros, los que serán aplicados por el área respectiva que solicita el servicio y asesorados por el departamento técnico de la compañía.

Por otra parte, el área de TI deberá verificar la existencia de planes de contingencia para efectos de validar superficialmente que estos cumplen de buena forma con el criterio de disponibilidad del servicio y los datos.

Para el caso de servicios asociados a tecnología y sistemas, será responsabilidad de la dirección de Monitoreo y gestión, incorporar en su control de monitoreo la disponibilidad de los servicios tecnológicos, plataformas de infraestructura y los sistemas de información que sean entregados por el proveedor, con la finalidad de medir los niveles del servicio y gestionar de manera oportuna cualquier incidente que puedan afectar el principio de disponibilidad.

En la medida que el área requirente necesite información detallada del servicio o sus equipos, podrá solicitar un informe técnico sobre la disponibilidad del servicio dentro de un período determinado, incluyendo el rendimiento de los equipos en caso que se haya sido acordado previamente entre las partes supervisar la capacidad de los sistemas.

Para facilitar el acceso a estas normativas de seguridad por parte de los proveedores, estas quedarán a libre disposición de quien lo requiera en el sitio Web de ASIC S.A.S. y la Intranet, considerando además el envío por correo electrónico a todos los funcionarios o asesores del servicio y su incorporación como referencia en las normativas asociadas a los procesos de compra.