NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

1. OBJETO

Establece la Normativa de Seguridad de la Información aplicable a los proveedores que presten servicios a la Autoridad Portuaria de Tarragona (en adelante APT).

2. ALCANCE

Proveedores de servicios de la APT.

3. LA SEGURIDAD DE LA INFORMACIÓN PARA LA APT

3.1. La información, así como las personas, los procesos, sistemas, redes, etc. que la soportan son considerados activos importantes. La disponibilidad, integridad, confidencialidad, autenticación y trazabilidad de la información, y de los activos que la soportan, son esenciales para mantener la seguridad de la información, el cumplimiento de la legalidad vigente, la competitividad, y la buena imagen para con los clientes.

Para lograr una adecuada seguridad de la información es imprescindible la gestión de la misma apoyándose en unas normativas y procedimientos adecuados a cumplir por todas las personas que actúan sobre activos de la APT en el desarrollo de sus funciones.

3.2. Objetivos de la Normativa de Seguridad de la Información

Los objetivos globales de la Normativa de Seguridad de la Información son los siguientes:

- Marco Jurídico

Se adquiere el compromiso de velar por el cumplimiento de la legislación vigente en materia de protección y seguridad de la información y de los sistemas aplicable a todos sus procesos de negocio.

- Marco Normativo

Cumplimiento de las obligaciones contractuales establecidas tanto con clientes como proveedores, en relación a la seguridad de la información.

Cumplimiento de los requisitos y buenas prácticas de Seguridad de la Información incluidas en las Normas ISO27001 e ISO27002.

4. ORGANIZACIÓN DE LA NORMATIVA, REVISIÓN Y ACTUALIZACIÓN

Esta normativa será revisada periódicamente. No obstante, debido a la propia evolución de la tecnología, las amenazas en relación a la seguridad de la información y a las nuevas obligaciones legales en la materia, la APT se reserva el derecho a modificar esta normativa cuando sea necesario. Los cambios realizados serán divulgados a todas las partes interesadas mediante la publicación en la página web de la APT y la notificación de la nueva versión mediante correo electrónico por parte del CAU. Es responsabilidad de todo el personal que desarrolle actividades para la APT, la lectura, conocimiento y cumplimiento de esta Normativa de Seguridad de la Información para proveedores.

5. INCUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

La APT se reserva el derecho adoptar las medidas que se consideren pertinentes en relación a la empresa contratada, y que pueden llegar a la resolución de los contratos que se tenga vigentes con dicha empresa.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Objetivos

Mantener la seguridad de la información sobre los activos de información de la APT que son objeto de acceso, tratamiento, comunicación o gestión por proveedores de servicio.

6.2. Proveedores

Los acuerdos (contratos) que impliquen acceder, procesar, comunicar o gestionar la información de la organización o los servicios de procesado de información, o añadir productos o servicios a los servicios de procesado de información, indicarán los controles de seguridad requeridos por parte de la APT previa a la prestación del servicio.

7. GESTIÓN DE ACTIVOS

7.1. Objetivos

- Establecer y mantener una protección adecuada a los activos de la APT
- Asegurar que la información recibe un nivel adecuado de protección

7.2. Responsabilidades sobre los activos

Se cumplirán, por parte del proveedor, las normas de uso aceptable de los activos establecidas por la APT en su gestión de la seguridad de la información.

7.3. Clasificación de la información

- Toda la información relacionada con las actividades de la APT se considera confidencial. El proveedor deberá cumplir las funciones y obligaciones aplicadas a la utilización de los sistemas de información según la normativa establecida por la APT.
- Se garantizará el manejo de la información de acuerdo al criterio de clasificación establecido.

8. SEGURIDAD FÍSICA Y AMBIENTAL

8.1. Objetivos

- Prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones e información de la APT.
- Proteger los sistemas de la APT, ubicándolos en áreas protegidas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
- Contemplar la protección de los sistemas de la APT en su traslado y permanencia fuera de las áreas seguras, por motivos de mantenimiento u otros.
- Controlar los factores externos o del entorno que pudieran perjudicar el correcto funcionamiento de los sistemas de información que albergan la información de la APT.
- Implementar medidas para proteger la información manejada por el personal, en el marco normal de sus labores habituales.

8.2. Áreas seguras

- Se utilizarán correctamente los controles físicos de entrada establecidos para asegurar que únicamente accede el personal autorizado a los espacios de los que dispone la APT: oficinas, despachos e instalaciones.
- Se seguirán las directrices y medidas de protección establecidas por la APT contra las posibles amenazas externas y de origen ambiental.
- Se cumplirán las directrices establecidas para trabajar en las áreas protegidas.
- Llevar la identificación mientras permanezcan en instalaciones de la APT.

8.3. Seguridad de los equipos

- La infraestructura tecnológica se ubicará en emplazamientos securizados y protegidos con el fin de reducir los riesgos derivados de las amenazas externas.
- Se protegerá la infraestructura tecnológica, que así lo necesite, contra fallos de provisión en el suministro eléctrico.

- La conexión de cualquier equipamiento a los circuitos tanto eléctrico como de comunicaciones estará previamente validado, con el fin de evitar interceptaciones o daños.
- Se deberá solicitar validación previa y se implementarán medidas de control indicadas, sobre toda la infraestructura que por necesidades puntuales se tenga que ubicar fuera de las áreas protegidas de la APT o fuera de la organización.
- Salvo en aquellos casos en que se reciba actualización expresa, se prohíbe sacar de las instalaciones cualquier infraestructura TIC o software propiedad de la APT.

9. GESTIÓN DE COMUNICACIONES Y OPERACIONES

9.1. Objetivos

- Garantizar el funcionamiento correcto y seguro de los activos que ofrecen los diferentes servicios a la APT.
- Establecer responsabilidades y facilitar procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta ante incidentes y separación de funciones.

9.2. Responsabilidades y procedimientos de operación

- La APT facilitará, en función de las necesidades identificadas, procedimientos de operación actualizados a los proveedores que los necesiten.
- Se prohíben los cambios sobre las infraestructuras y los recursos.
- Se definirán áreas de responsabilidad y tareas de manera segregada en los contratos de relación y en los acuerdos de nivel de servicio que se establezcan, con el fin de evitar modificaciones no autorizadas.
- Se deberá garantizar, en función del servicio prestado por el proveedor, la utilización correcta de los entornos de desarrollo y pruebas.

9.3. Gestión de la provisión de servicios

- Se realizarán por parte de la APT, controles para verificar que los requerimientos de seguridad establecidos de forma previa a la prestación de servicio han sido implementados y se mantienen en el tiempo correctamente.
- Los servicios prestados serán supervisados y revisados periódicamente. En función del tipo de servicio se podrán establecer auditorías de cumplimiento.
- En función de la criticidad y/o riesgo del servicio contratado, los cambios en la provisión del mismo deberán ser validados previamente por la APT.

9.4. Planificación y aceptación del sistema

- Se establecerá una supervisión de la utilización de los recursos propiedad de la APT empleados por el proveedor, con el fin de garantizar una correcta capacidad de los mismos tanto en el presente mediante su monitorización, como en el futuro mediante el análisis de tendencias.
- Se establecerán criterios de aceptación para nuevos sistemas o la modificación de los existentes, realizadas por proveedores. En los entornos de desarrollo y prueba se realizarán las pruebas que garanticen un correcto paso al entorno de producción. Únicamente tras una aceptación formal se migrará al entorno de producción.

9.5. Protección contra código malicioso y descargable

Se prohíbe la ejecución de código no autorizado. La configuración de los equipos garantizará que el código autorizado funciona de acuerdo con lo definido en la normativa establecida al respecto.

9.6. Gestión de la seguridad de las redes

- No se evitarán los mecanismos y actividades de gestión establecidos por la APT que permitan proteger frente a las amenazas que les puedan afectar las redes y a las aplicaciones que las utilizan.
- Se identificarán tanto las características de seguridad, los niveles de servicio y los mecanismos de gestión para garantizar la seguridad del servicio de red prestados por proveedores.

9.7. Manipulación de los soportes

- La utilización de soportes extraíbles de información deberá ser validada previamente por la APT y con la finalidad exclusiva recogida en el contrato de relación.
- A la finalización de la relación contractual con la APT, los soportes extraíbles facilitados al proveedor para el desarrollo de sus funciones, deberán ser devueltos.
- El uso y almacenamiento de información en soportes extraíbles y la manipulación de los soportes estará regulado mediante la normativa establecida en la APT.
- Se prohíbe el acceso a la documentación de la APT, ubicada tanto en repositorios automatizados como no automatizados, a la que no se haya dado acceso expreso para el fin descrito en la prestación del servicio contratado.

9.8. Intercambio de información

- Sobre los intercambios de información realizados entre el proveedor de servicio y la APT se establecerán, en función de la criticidad considerada por la APT,

- controles normativos, procedimentales y técnicos que protejan el intercambio de dicha información.
- El intercambio de información y el tratamiento de la misma, quedará regulado mediante el correspondiente acuerdo o contrato de relación entre la APT y el proveedor receptor de la misma.
- En los casos en los que la prestación del servicio incluya el tránsito de información, se implementarán por parte del proveedor los controles normativos y técnicos que eviten el uso indebido o el deterioro de la misma. La APT se reservará el derecho de auditar estos controles o requerir la implantación de protecciones adicionales.
- La APT podrá requerir que la información transmitida mediante mensajería electrónica esté adecuadamente protegida por parte del proveedor, requiriendo el cumplimiento de una normativa específica y/o la implementación de controles técnicos auditables.
- Se prohíbe la transmisión de información de la APT a otras organizaciones. En caso de necesidad para la prestación del servicio contratado, el proveedor de servicio deberá solicitar a la APT validación previa a la transmisión de dicha información. En función de los niveles de clasificación y los requerimientos legales establecidos, la APT solicitará controles de seguridad específicos y que podrán ser auditados.

9.9. Supervisión

- La APT dispondrá de elementos de monitorización que permitan la auditoría de las actividades, las excepciones y eventos de seguridad del proveedor en función de las necesidades de la organización, disponiendo de estos registros durante el tiempo que se considere con el fin de servir como prueba forense y/o en la supervisión del control de accesos.
- Se supervisará el uso de los sistemas de información, por parte del proveedor y esta información se tratará periódicamente.
- Las actividades de administración y operación que pudieran ser realizadas por parte del proveedor de servicio sobre los sistemas de información de la APT, serán registradas.

10. CONTROL DE ACCESO

10.1. Objetivos

- Impedir el acceso no autorizado a la información y los sistemas de información.
- Implementar seguridad en los accesos del proveedor por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la APT y otras redes públicas o privadas.

- Registrar y revisar eventos y actividades críticas llevadas a cabo por el proveedor en los sistemas.
- Concienciar al proveedor respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan portátiles e instalaciones remotas.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.

10.2. Requisitos de la APT para el control de acceso

El proveedor únicamente tendrá acceso a aquellos recursos de red, aplicaciones e información que sean necesarios para el desempeño de las labores propias del servicio contratado. Los derechos de acceso a las mismas serán los mínimos posibles en función de dichas necesidades. Las reglas de control de accesos se establecerán de acuerdo a la “necesidad de saber”.

10.3. Gestión de acceso de usuario

- Todo proveedor, previa a la prestación y a la finalización del servicio en la APT, deberá solicitar el alta y baja de usuarios en base al procedimiento formal de registro y anulación de usuarios que concede y revoca el acceso a los sistemas de información.
- Todo cambio en la prestación del servicio que suponga cambio en las personas que participan en el mismo deberá ser notificada a la mayor brevedad a la APT con el fin de realizar las bajas y altas correspondientes. La APT se reserva el derecho de auditar periódicamente las asignaciones realizadas.

10.4. Responsabilidades del usuario

- Se requerirá al proveedor el uso de buenas prácticas de seguridad en la selección y uso de contraseñas sobre sus sistemas de información, sobre todo en aquellos que no dispongan de políticas automáticas de calidad de contraseña.
- Se requerirá al proveedor el puesto de trabajo despejado de papeles y de soportes de información si no se están utilizando y la ocultación de información de la pantalla del equipo si no se está delante.

10.5. Control de acceso a red

- Se proporcionará al proveedor acceso a los servicios de red requeridos para la prestación del servicio contratado.
- Las conexiones externas de un proveedor a infraestructuras de la APT, deberán ser previamente validadas. En función del análisis del riesgo de la conexión, se requerirán controles de seguridad auditables.

- Se prohíbe el acceso físico y lógico a los puertos de diagnóstico y de configuración de las infraestructuras de la APT. En caso de requerirse por definición del servicio, se registrarán dichos accesos.
- En base a la arquitectura de red segregada, las conexiones a las mismas se realizarán en función de las necesidades concretas de conectividad para la prestación del servicio. Se prohíbe la configuración de rutas o accesos no validados previamente por la APT.

10.6. Control de acceso a los sistemas operativos

- Para el equipamiento de usuario, el acceso a los sistemas operativos requerirá inicio de sesión válido sobre el dominio de la APT si así lo exige el servicio. Para los servidores y equipamiento de comunicaciones se requerirá la asignación específica de funciones de administración. En los casos en los que lo exija el servicio.
- Todos los usuarios dispondrán de identificador único de usuario para su uso personal y exclusivo.
- Se prohíbe de manera explícita el uso de aplicaciones y/o utilidades que pudieran invalidar los controles de acceso y/o aplicación y las no asociadas a la prestación del servicio contratado.
- Sobre los sistemas de información sobre los que se identifiquen niveles de riesgo extraordinarios se utilizarán restricciones en los tiempos de conexión.

10.7. Control de acceso a las aplicaciones y a la información

El acceso a la información será restringida en función a su necesidad de conocer para los servicios contratados a cada proveedor.

11. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

11.1. Objetivos

- Cumplir los controles de seguridad en el ciclo de vida de los sistemas de información.
- Cumplir las normas y procedimientos que se aplican durante el ciclo de vida de las aplicaciones y en la infraestructura de base en la cual se apoyan.
- Regular el uso de información confidencial.
- Garantizar el procesamiento correcto de las aplicaciones.
- Garantizar el uso correcto de la información en los distintos entornos de desarrollo, prueba y producción.
- Minimizar las vulnerabilidades técnicas.

11.2. Requisitos de seguridad de los sistemas de información

Previa a la contratación y/o adquisición de nuevos servicios se realizará un análisis previo en relación a la seguridad de la información por parte de la APT. Si se considera oportuno, se incluirán requerimientos específicos en esta materia junto a los requisitos funcionales.

11.3. Tratamiento correcto de las aplicaciones

- Se establecerá la validación de los datos de entrada en las aplicaciones desarrolladas con el fin de garantizar que los mismos son correctos y adecuados.
- Sobre las aplicaciones desarrolladas se establecerán controles de procesamiento interno que permitan la detección de cualquier modificación de la integridad de la información tanto por error como de manera intencionada.
- Se establecerán controles de seguridad que garanticen los mecanismos de comunicación entre procesos, la autenticación e integridad de los mensajes.
- Se establecerán controles para la validación de datos de salida de las aplicaciones que permitan garantizar que la información almacenada es correcta y adecuada.
- Se aplicara la sistemática de Desarrollo y Mantenimiento de aplicaciones existente en la APT (procedimientos, instrucciones técnicas y formatos).

11.4. Controles criptográficos

- El cifrado de información seguirá los requerimientos establecidos por la APT para el cumplimiento de requisitos legales y de negocio, empleando algoritmo de cifrado fuerte que no padezca vulnerabilidades ni debilidades conocidas y utilizando una herramienta informática adecuada para la utilización del algoritmo y clave.
- Las claves criptográficas utilizadas por parte del proveedor estarán protegidas contra modificación, pérdida y destrucción. Se tendrá en cuenta la autenticidad de las claves públicas empleadas. El proceso de autenticación se llevará a cabo utilizando certificados de clave pública expedidos por una autoridad de certificación reconocida que contará con los controles y procedimientos adecuados para ofrecer el grado de confianza necesario.

11.5. Seguridad de los archivos del sistema

- Se utilizarán los procedimientos de los que se dispone en la APT para la instalación y actualización de software en los entornos de producción.
- Se evitarán el uso de datos reales en el entorno de pruebas. En caso de recurrir a datos de este tipo, el proveedor deberá disponer de la correspondiente validación por parte de la APT y previa a su utilización en el entorno de pruebas se garantizará la disociación de dicha información. En todo

- caso la información utilizada para pruebas estarán en todo momento protegida y controlada.
- El acceso al código fuente de los programas y a los elementos relacionados con él (diseños, especificaciones, planes de verificación y validación) estarán estrictamente controlados por la APT, para evitar cambios involuntarios o la introducción de funciones no autorizadas.

11.6. Seguridad en los procesos de desarrollo y soporte

- Previos a la introducción de nuevos sistemas o de cambios importantes en los ya existentes, el proveedor seguirá el proceso de gestión de cambios establecido en la APT.
- Se evitarán las situaciones que permitan que se produzcan fugas de información. El proveedor tendrá la obligación de notificar a la APT a la mayor brevedad estas situaciones.
- El desarrollo realizado por el proveedor será supervisado y controlado por la APT en base a los requerimientos previamente establecidos en el correspondiente contrato de relación.

11.7. Gestión de las vulnerabilidades técnicas

Las vulnerabilidades técnicas identificadas en los sistemas de información no serán explotadas por el proveedor de servicios. Serán notificadas a la mayor brevedad a la APT.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

12.1. Objetivos

- Establecer canales de comunicación de eventos y debilidades relativos a la seguridad de la información.
- Gestionar los incidentes de seguridad.
- Aprender de los incidentes de seguridad.

12.2 Notificación de eventos y puntos débiles de la seguridad de la información

- El proveedor estará obligado a notificar cualquier incidente de seguridad que se produzca en la prestación del servicio. Esta notificación deberá realizarse a la mayor brevedad a través del centro de atención al usuario (CAU) a la dirección de correo sgsi@porttarragona.cat. Se emplearán además los elementos de supervisión, alertas y vulnerabilidades de que se dispone para detectar incidentes de seguridad de la información.

- Cualquier punto débil, en relación a la seguridad de la información, deberá ser notificado a través del centro de atención al usuario (CAU) a la dirección de correo sgsi@porttarragona.cat. No se deberá intentar comprobar ningún punto débil de seguridad que se sospeche que exista.

12.3. Gestión de incidentes de seguridad de la información y mejoras

- Todos los incidentes de seguridad serán gestionados por la APT y podrán requerir la colaboración del proveedor para su resolución.
- En base a la gestión anteriormente indicada se dispondrá de información que permita su explotación para el análisis y aprendizaje de las partes implicadas.
- Las evidencias recopiladas en la gestión de un incidente de seguridad podrán ser requeridas por el órgano judicial competente por lo que serán convenientemente almacenadas y custodiadas.

13. GESTIÓN DE LA CONTINUIDAD DE LA APT

13.1. Objetivos

- Establecer las pautas de actuación a seguir para garantizar la continuidad de los procesos de negocio.
- Establecer las pautas a seguir para llevar a cabo la activación y desactivación del plan.

13.2 Aspectos de seguridad de la información en la gestión de la continuidad de la APT

- Los planes de contingencia derivados del plan de continuidad de negocio, que permiten mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y tiempo requerido, pueden requerir la intervención de proveedor de servicio.
- El plan de continuidad de negocio y los planes de contingencia derivados serán probados y actualizados periódicamente para asegurar su efectividad. Se garantizará que todos los miembros de los equipos de recuperación, así como cualquier proveedor afectado, conoce sus responsabilidades.

14. CUMPLIMIENTO

14.1. Objetivos

- Cumplir con las disposiciones legales, normativas y contractuales a fin de evitar sanciones administrativas a la APT y/o al empleado, o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

- Garantizar que el proveedor cumplan con la política, normas y procedimientos de seguridad de la APT.
- Revisar la seguridad del proveedor de la APT periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información utilizados para la prestación.
- Optimizar la eficacia del proceso de auditoría sobre el proveedor de servicio.

14.2. Cumplimiento de los requerimientos legales

- El proveedor garantizará el cumplimiento de la normativa establecida en relación al uso de material sobre el que puedan existir derechos de propiedad intelectual.
- El proveedor velará por la protección de los activos de la APT frente a distintas amenazas, durante el tiempo y forma que se establezca en la relación contractual, en base a los requerimientos legales, reglamentarios y empresariales.
- El proveedor garantizará el cumplimiento de los requerimientos establecidos por el RGPD. Del mismo modo, el proveedor asignado como encargado de tratamiento de ficheros de la APT con datos de carácter personal cumplirá los requerimientos establecidos por la APT como propietario de dichos ficheros.
- La presente Normativa de Seguridad de la Información para proveedores así como la derivada de la misma constituyen elementos que previenen el uso indebido tanto de la información como de los recursos de tratamiento de la información.

14.3. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

- El proveedor se asegurará, dentro de su ámbito, del cumplimiento de las normativas establecidas en relación a la seguridad de la información. El resultado de las revisiones de cumplimiento y las acciones correctivas derivadas constituirán evidencias de gestión de la seguridad de la información en cada ámbito de responsabilidad, a considerar en las revisiones de la provisión.
- En función del servicio contratado y las necesidades de la APT, se realizarán comprobaciones de cumplimiento técnico sobre los recursos de tratamiento de la información, en base a la normativa establecida en la APT para la gestión de la seguridad de la información.

14.4. Consideración sobre la auditoría de los sistemas de información

- Las auditorías de cumplimiento serán previamente planificadas con el fin de evitar riesgos sobre los activos de la APT y los servicios prestados.

- Tanto las herramientas de auditoría como los registros obtenidos en el proceso se mantendrán en entornos diferentes a los de desarrollo u operativos con el fin de evitar cualquier peligro o uso indebido. Si en la auditoría participa o la realiza enteramente un proveedor, se podrá considerar la evaluación del riesgo previo que esto suponga y el requerimiento de controles de seguridad específicos sobre el proveedor.

15. AUDITORIA

A requerimiento de la APT, se podrán realizar auditorías de cumplimiento sobre los puntos indicados, con el fin de determinar el grado de cumplimiento de la Normativa de Seguridad de la Información para proveedores y establecer acciones correctivas en su caso.

DOCUMENTOS RELACIONADOS:

Código de Conducta Informático para Proveedores