S-IT-01-00-28 – Política de requisitos de ciberseguridad para el suministro o la prestación de servicios

Clasificación de la Información:

Nivel del Documento	Documentación General
Nombre del Fichero	S-IT-01-00-28 -PolíticaCiberseguridadConTerceros.docx
Tipo	DIFUSIÓN LIMITADA
Ámbito de Difusión	PUBLICA
Responsable	Responsable de Seguridad de la Información

CONTROL DE MODIFICACIONES				
Fecha	**Versión**	**Descripción**	**Revisado**	**Aprobado**
01/10/2022	1.0	Versión preliminar del documento	Responsable de seguridad	Dirección

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

El objetivo principal de este documento es mitigar los riesgos posibles asociados al acceso a la información, sistemas de información o recursos de PLASTIC7A.

NOTA: Este documento es una versión reducida y PÚBLICA del documento S-IT-01-00-28 - PolíticaCiberseguridadConTerceros y por tanto solo es una referencia mínima del contenido desarrollado en el documento principal.

2. OBJETO

Definir los requisitos de Ciberseguridad que deben quedar asegurados en todas las actividades que afectan al satisfactorio comportamiento en el suministro o el servicio.

3. APLICABILIDAD

Los requisitos de Ciberseguridad serán de aplicación para por parte de proveedores de servicios, independientemente del tipo de servicio proporcionado, o de relación que le una con PLASTIC7A (legal, contractual o de cualquier otra índole no laboral), con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de PLASTIC7A y sus clientes. Lo que incluye, pero no se limita, a peticiones de oferta o provisiones o prestaciones de Sistemas Digitales, Montaje/Pruebas, Cambios de Diseño, Servicios y Materiales.

4. REFERENCIAS

- S-IT-01-00-00-PoliticaDeSeguridadTIC.

5. REQUISITOS DE CIBERSEGURIDAD

5.1 Confidencialidad

La relación con empresas de suministros y/o servicios que tengan acceso a información sobre Sistemas Digitales, debe estar regulada mediante contratos o cláusulas de confidencialidad.

Toda información, documentación, programas y/o aplicaciones, métodos, organización, estrategias de negocio y actividades relacionadas con PLASTIC7A o con su negocio, a las que tenga acceso los proveedores de servicios con objeto de realización del servicio serán considerados información confidencial, en función de lo cual, el acceso, intercambio y tratamiento de dicha información, se realizará siempre de acuerdo a las finalidades previstas descritas en el contrato de prestación de servicios y manteniendo el correspondiente deber de secreto durante la duración del servicio y después de que finalice la relación con PLASTIC7A.

Todos los recursos e información a la que haya podido tener acceso o que haya sido necesaria elaborar, modificar o copiar para el correcto desempeño del servicio serán devueltos a la finalización de este. PLASTIC7A podrá solicitar el borrado seguro de los dispositivos que hayan tenido acceso a la Información de PLASTIC7A.

Siempre que la prestación de servicios suponga el acceso de personal externo a Sistemas Digitales o a información confidencial de PLASTIC7A, se considerarán cláusulas y contratos de confidencialidad en la contratación.

5.2 Intercambios de información

Cualquier tipo de intercambio de información que se produzca entre PLASTIC7A y los proveedores de servicios se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

PLASTIC7A se reserva, en función del riesgo identificado, la implantación de medidas de control, registro y auditoría sobre estos recursos de difusión.

5.3 Fiabilidad

Los suministradores de productos o servicios de Sistemas Digitales deben asegurar por contrato que los productos adquiridos por PLASTIC7A están libres de vulnerabilidades comprobables y código malicioso conocido.

Si un suministrador detecta una vulnerabilidad en su producto, debe comunicarlo inmediatamente a PLASTIC7A, ya sea en la fase de diseño, implantación o explotación.

Se requiere que los productos adquiridos dispongan de embalajes, precintos o sellos a prueba de manipulaciones.

5.4 Uso de los recursos corporativos de PLASTIC7A

Los recursos corporativos de PLASTIC7A a los que tengan acceso los proveedores de servicios serán utilizados exclusivamente para cumplir con las obligaciones y propósitos de la provisión del servicio.

Bajo ningún concepto podrán ser utilizados para actividades no relacionadas con el propósito del servicio.

5.5 Responsabilidades del usuario

Los Proveedores de servicios deberán asegurarse de que todo el personal que en el desarrollo de sus funciones para PLASTIC7A puedan tener acceso a la información, sistemas de información o recursos de PLASTIC7A respete los siguientes principios básicos dentro de su actividad

5.6 Requisitos de seguridad para los dispositivos

Todos los dispositivos con acceso a información de PLASTIC7A, independientemente de la propiedad de estos, deberán cumplir con las políticas de seguridad establecidas por PLASTIC7A

5.7 Comunicación de incidentes de seguridad

Los proveedores de servicios se comprometen a comunicar de manera inmediata cualquier incidente, debilidad o amenaza (observada o sospechada) que detecte en los sistemas de información de PLASTIC7A o que haya podido afectar a información propiedad de PLASTIC7A o de sus clientes al Departamento de Seguridad de la Información a través del Usuario Genérico PLASTIC7A CSIRT ciberseguridad@plastic7a.com, o a través del Responsable del servicio.

En el caso de personal del proveedor desplazado en PLASTIC7A, cualquier incidente, debilidad o amenaza relacionada con la información o los recursos de PLASTIC7A deberá ser comunicada a través del Usuario Genérico PLASTIC7A CSIRT ciberseguridad@plastic7a.com o del centro de atención al usuario (CAU) de PLASTIC7A.

5.8 Principios específicos de seguridad

5.8.1 Seguridad física

Obligados: Todos los proveedores de servicios cuyos servicios se presten desde la sede del proveedor.

- Los edificios o instalaciones deben ser físicamente sólidos (por ejemplo: no deberían existir huecos en el perímetro o áreas dónde pudieran producirse rupturas fácilmente); los muros externos de las instalaciones deberían ser de construcción sólida.
- Todas las puertas externas deberían estar adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control, por ejemplo, barras, alarmas, cerraduras, tornos, cámaras de vigilancia etc.
- Cuando sea posible, se recomienda establecer barreras físicas que requieran la identificación del empleado mediante algún método de identificación y autenticación (tarjetas de identificación, tarjetas electrónicas, identificación biométrica, etc.) para prevenir los accesos físicos no autorizados.
- Los edificios o instalaciones deberían contar con sistemas automáticos de detección y respuesta automática ante condiciones ambientales adversas (fuego principalmente). Cuando no se pueda disponer de un sistema de extinción automática de incendios, deben contarse con medidas de extinción manual, que deben ser conocidas por todo el personal de la empresa.
- Se deben establecer las condiciones ambientales básicas de temperatura, higiene, aislamiento eléctrico y sonoro, y otras medidas similares de acuerdo con los requerimientos específicos del equipamiento informático.
- Si se mantiene algún tipo de copia de información responsabilidad de PLASTIC7A, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las siguientes medidas de seguridad:
    - Tener un sistema de control de acceso independiente al de la sede.
    - Existirá un registro de acceso realizados.
    - El acceso por parte de personal externo se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado.
    - El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.

- Contar con algún tipo de protección frente a fallos de alimentación.

5.8.2 Seguridad en desarrollo

Obligados: Todos los proveedores de servicios que realicen trabajos de desarrollo y/o pruebas de aplicaciones para PLASTIC7A.

- Los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción.
- Todos los accesos a los sistemas de información que alberguen o procesen información deberán estar protegidos, al menos, por un "cortafuegos", que limite la capacidad de conexión a ellos.
- Todo el proceso de desarrollo de software externalizado será controlado y supervisado por PLASTIC7A.
- Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.
- Se incorporarán los mecanismos de identificación, autentificación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implantación y operación de los aplicativos.
- Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.
- Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.
- Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
- Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.
- El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.
- En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.

- Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.
- Solo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

5.8.3 Seguridad de sistemas

Obligados: Todos los proveedores de servicios cuyos servicios se presten mediante el uso de su infraestructura TIC.

Gestión de activos

- Los proveedores de servicios deberán contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.
- Los proveedores de servicios deberán notificar a PLASTIC7A las bajas de los activos utilizados para la prestación del servicio. Si dicho activo contiene otra propiedad de PLASTIC7A (hardware, software u otro tipo de activos), deberá ser entregado a PLASTIC7A previamente a llevar a cabo la baja para que PLASTIC7A proceda a la retirada de los activos de su propiedad.
- Siempre que un activo haya contenido información considerada sensible, Los Proveedores de servicios deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable.
- Todos los activos utilizados para la prestación del servicio deberán tener un responsable, que se deberá asegurar de que dichos activos incorporan las medidas de seguridad mínimas establecidas por PLASTIC7A, y que al menos deben ser las especificadas en la presente normativa:
- Cumplir lo establecido en el punto Requisitos de seguridad para los dispositivos.
- El Proveedor establecerá una normativa de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad semanal.

Gestión de la continuidad

- Los proveedores de servicios deberán contar con un plan de continuidad y un plan para la recuperación de TI en caso de desastre que permita la prestación del servicio aun en caso de contingencias. Este plan deberá ser desarrollado en función de una evaluación de riesgos (al menos una vez al año) para identificar los riesgos que podrían causar una interrupción de las operaciones y asegurarse de que se ponen en funcionamiento los controles apropiados para gestionarlos y controlarlos.
- Los proveedores de servicios pondrán a prueba el plan de continuidad y el plan de recuperación para confirmar que sirven para recuperar el servicio en los plazos de tiempo

acordados. Estas pruebas se realizarán anualmente o justo después de que se realicen cambios, mejoras o modificaciones importantes que afecten a los servicios.

Seguridad de red

- Todas las redes deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por él, estableciéndose los oportunos sistemas de monitorización y auditoría de seguridad necesarios para garantizar la seguridad de las conexiones.
- Los servicios disponibles en las redes a través de las que circule la información deberán limitarse en la medida de lo posible.
- Las redes que permitan el acceso a la infraestructura PLASTIC7A deberán estar apropiadamente protegidas.

Gestión de cambios

- Los Proveedores de servicios deberán garantizar que todos los cambios en la infraestructura TIC con la que presta el servicio están controlados y autorizados, garantizándose que no forma parte de la infraestructura TIC ningún componente no controlado.
- Se deberán verificar que todos los nuevos componentes introducidos en la infraestructura TIC utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.
- Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.
- El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre los componentes críticos, limitándose a los estrictamente imprescindibles.
- Se deberán verificar todos los cambios sobre los componentes críticos, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento de dichos componentes o sobre su seguridad.
- Se deberán analizar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a PLASTIC7A de todas aquellas asociadas a los componentes críticos, con el fin de gestionar conjuntamente dichas vulnerabilidades.

6. ANEXOS.

Ver documentos adicionales.

- Documento Notificación Estado de Ciberseguridad: S-IT-01-00-28-04-NOTIFICACION
- Documento e Confidencialidad: S-IT-01-00-28-03-ACUERDO DE CONFIDENCIALIDAD