OPENSERVICES

CONSULTORIA EN TRANSPORTES

POLÍTICA DE SEGURIDAD

Índice de contenido

Introducción

OPENSERVICES, como cualquier otra organización basada en la información, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. De la operatividad de estos servicios, surge la necesidad de proteger la información y los servicios prestados frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad. Todo ello, con el compromiso de un equilibrio entre la seguridad y su coste, tanto económico, como operativo.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Para ello, esta Política de Seguridad de la Información, define la estructura básica de la organización de seguridad en OPENSERVICES, así como los principios básicos para la implementación de las medidas técnicas y organizativas de seguridad que se desarrollan en normas y procedimientos de seguridad del Ministerio.

Dado que el entorno tecnológico es muy variable, se requiere una estrategia que se adapte a los cambios en las condiciones que garanticen la prestación continua de los servicios. Por ello, los distintos departamentos aplican las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizan un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. Debemos estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del Esquema Nacional de Seguridad.

La seguridad TIC debe ser considerada asimismo en cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Se requiere cada vez mayor interconexión de los sistemas de información de OPENSERVICES con otros sistemas de la Administración pública o del sector privado. Se produce por ello, un aumento de los riesgos inherentes a la exposición a entornos fuera del control de los propietarios de los sistemas. Esta Política de Seguridad de la Información busca establecer los principios básicos y requisitos mínimos de seguridad que permitan operar los sistemas de información de OPENSERVICES dentro de un rango aceptable de riesgo para la confidencialidad e integridad de sus datos y la disponibilidad de los mismos.

OPENSERVICES debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

Prevención

OPENSERVICES debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

OPENSERVICES:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Recuperación

Para garantizar la disponibilidad de los servicios críticos, OPENSERVICES dispondrá de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

1.1 Conceptos Generales

Se describen a continuación los conceptos generales en materia de seguridad de la información:

- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Utilidad**: Los recursos del sistema y la información manejada en el mismo han de ser útiles para alguna función.

- **Integridad**: Propiedad de la información relativa a su exactitud y completitud. La información del sistema ha de estar disponible tal y como se almacenó por un agente

autorizado.

- **Autenticidad**: El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

- **Posesión**: Los propietarios de un sistema han de ser capaces de controlarlo en todo momento y ser responsables del mismo.

El Esquema Nacional de Seguridad sigue los mismos pasos que un SGSI basado en el ciclo de Deming, conocido como PDCA, en el cual se establecen las fases:

- **P (Planificar):** establecimiento de las actividades, responsabilidades y recursos además de los objetivos a cumplir y cómo se van a medir estos objetivos.

- **D (Desarrollar):** desarrollo e implementación de los procesos. Una vez implementados, medición de los resultados de la ejecución de dichos procesos.

- **C (Comprobar):** análisis de los resultados para comprobar si se han alcanzado los objetivos y si no es así, identificar las causas.

- **A (Actuar):** ejecución de las acciones necesarias para corregir los aspectos de mejora de detectados en los procesos o para mejorarlos.

1.2 Contexto de la Entidad

OPENSERVICES ha tomado la decisión de implantar el ENS, contando para ello con el compromiso e implicación de la Dirección, y teniendo en cuenta las diferentes partes implicadas en el sistema de información siendo estas principalmente:

- **Clientes.** Como parte fundamental del sistema, se velará por preservar la confidencialidad, integridad y disponibilidad, de la información intercambiada con los clientes, y necesaria para la prestación de los servicios, así como cualquier otra información (administrativa, de contacto…) necesaria para la prestación del servicio.
- **Proveedores.** Debido a la relevancia de los proveedores de servicios para el tratamiento de la información, especialmente en cuanto a los servicios de TI necesarios para la prestación de los servicios de OPENSERVICES (como son los proveedores de los servicios de redundancia), se han establecido los requisitos necesarios para garantizar la seguridad y disponibilidad de sus servicios. Se deben de tener en cuenta igualmente los envíos de información realizados a las entidades bancarias.
- **Administración Pública.** Como destinatarios de parte de la información de los usuarios y asociados, como consecuencia de los servicios prestados por OPENSERVICES, con la finalidad de cumplir con las normas y leyes de aplicación, y como responsables de los servicios asignados a la empresa. El envío de información se realizará, bien a través de los medios que dichos organismos ponen a disposición para tal fin (servicios web) o bien

mediante medios alternativos como correo electrónico (mediante firma electrónica) o soportes magnéticos.

- **Trabajadores.** Como parte fundamental en el tratamiento de la información, los empleados deberán de conocer las normas y procedimientos de seguridad que se decidan aplicar en la organización para asegurar la confidencialidad, integridad y disponibilidad de los datos.

1.1.1 Identificación de la legislación aplicable

Según la legislación vigente, las leyes aplicables a OPENSERVICES en materia de Seguridad de la Información son:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales

LOPD y Reglamento de desarrollo: OPENSERVICES cumple con las obligaciones establecidas en la LOPD, para lo que ha procedido a:

- Inscribir los ficheros en la Agencia de Protección de Datos
- Elaborar un Documento de Seguridad que define las responsabilidades, normas y procedimientos aplicables en materia de protección de datos de carácter personal.
- Implantar las medidas de seguridad de acuerdo a los niveles de seguridad de los ficheros gestionados.
- Firmar los contratos de encargado del tratamiento con cada una de las entidades que requieren el acceso a datos de carácter personal durante la prestación de servicios contratados.
- Elaborar las cláusulas informativas necesarias para informar a los afectados en el

momento de la recogida de datos de carácter personal.

- Definir los mecanismos para facilitar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición.

- Realizar auditorías, al menos cada dos años, que verifiquen el cumplimiento de lo dispuesto en la LOPD y su reglamento de desarrollo.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Ley de Propiedad Intelectual: OPENSERVICES cumple con las obligaciones establecidas en la Ley de Propiedad Intelectual, para lo que ha procedido a:

- Adquirir las licencias de uso necesarias para el software utilizado en el desarrollo de la actividad.

- Implantar los mecanismos necesarios para controles el uso y la necesidad de licencias.

Ley de servicios de la sociedad de la información y de comercio electrónico (LSSI): OPENSERVICES cumple con las obligaciones establecidas en la LSSI, para lo que ha procedido a:

- Adaptar el contenido de sus páginas web a los requisitos fijados por la norma.

1.1.2 Normas de Referencia

Las normas de referencia para la implantación del Sistema de Gestión de Seguridad de la Información son las siguientes:

- **Norma UNE/ISO-IEC 27001 Tecnología de la Información**. Especificaciones para los Sistemas de Gestión de Seguridad de la Información, en la que se recogen los requisitos para establecer, implantar, documentar y evaluar un SGSI. Es la norma sobre la que se desarrolla el sistema y la que permite obtener la certificación del mismo por parte de un organismo certificador independiente.

- **Norma UNE/ISO-IEC 27002 Tecnología de la Información**. Código de buenas prácticas para la Gestión de la Seguridad de la Información. Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad y constituir una práctica eficaz de la gestión.

1.1.3 Requisitos contractuales

No se han identificado requisitos adicionales exigidos por las empresas asociadas o por otras partes interesadas.

2. Esquema Nacional de Seguridad

2.1 Alcance

El alcance de la implantación del Esquema Nacional de Seguridad en OPENSERVICES, considera los siguientes servicios:

- Gestión de los datos del tacógrafo digital de los clientes de la empresa.

Prestado desde sus oficinas en:

Pl. Ind. Espíritu Santo, c/ Holanda, 1 - 2º A Oficina 1, 33010 Oviedo, Asturias

2.2 Descripción de servicios

A continuación se incluye una descripción de los servicios:

- **Gestión de los datos del tacógrafo digital de los clientes de la empresa.**
  - Por medio de la aplicación Opentach y Fich@: un servicio de análisis, gestión y alojamiento de los datos de los tacógrafos digitales que cumple con los requisitos técnicos especificados en el Reglamento CEE 3281/85.
  - **Desarrollo e implantación de herramientas de gestión y asistencia e intervención en procesos legales.** La empresa está integrada por un equipo de profesionales que están especializados, por un lado en el ámbito Informático y de Programación y desarrollo de programas tecnológicos y, por otro, en el ámbito del Derecho Administrativo y Derecho Penal, en lo que se refiere al transporte de mercancías y viajeros por carretera, así como en Seguridad Vial.

2.3 Declaración de la política de seguridad de la información

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de administración electrónica de OPENSERVICES.

Es la política de esta entidad asegurar que:

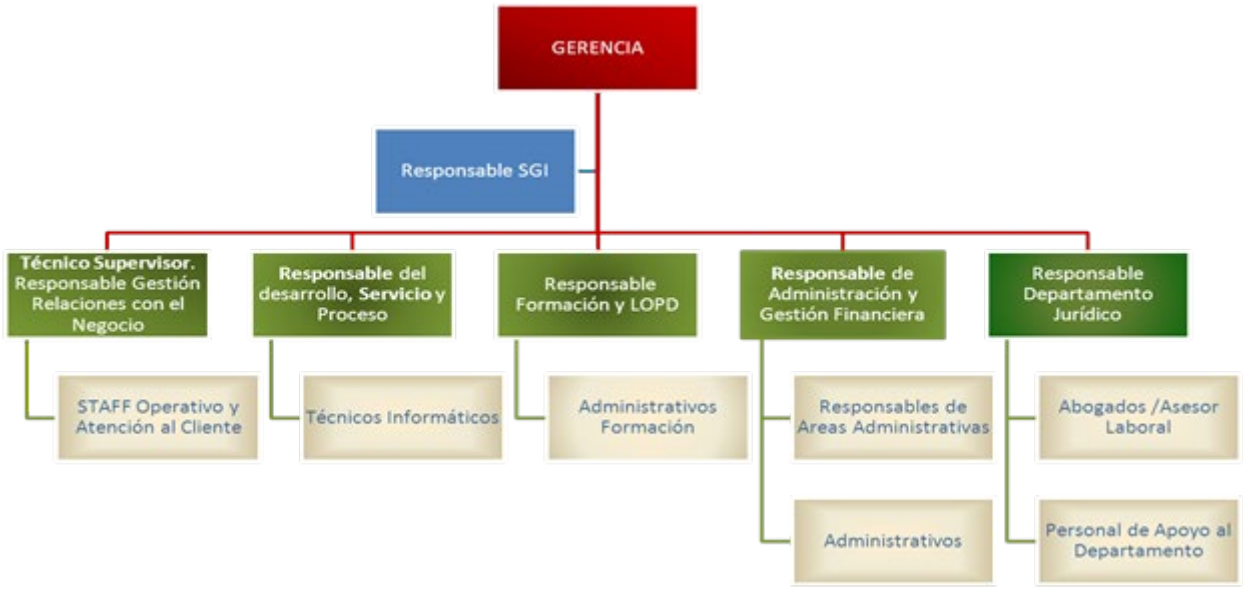
- La información y los servicios están protegidos contra pérdidas de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.
- La información está protegida contra accesos no autorizados.
- Su cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con esta Política.
- El Responsable de Seguridad de la Información será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.
- El Responsable de Servicio será el encargado de implementar esta Política y sus correspondientes procedimientos.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto.

- Es política de OPENSERVICES implementar, mantener y realizar un seguimiento del Esquema Nacional de Seguridad.

La Dirección de OPENSERVICES, se compromete a liderar este proceso y a asignar los recursos necesarios para cumplir con los requisitos establecidos en el Sistema de Gestión de Servicios de TI, satisfacer las exigencias de los clientes y conseguir los objetivos fijados.

La presente política es conocida y suscrita por todo el personal de OPENSERVICES contemplado en el alcance, de acuerdo a las exigencias de la Dirección. Esta política será revisada con una periodicidad máxima anual, y sus cambios deberán ser aprobados por la Dirección General de la organización.

2.4 Organigrama



2.5 Compromiso de la Dirección

La presente Política de Seguridad de la Información es una línea de actuación clara, manifiesta y pública de OPENSERVICES, por lo que la Dirección expresa su apoyo total a la misma y se compromete a mantener las directrices fijadas en el presente documento.

Asimismo, publicará y entregará a todos sus empleados y de la forma más apropiada el presente Documento, para que todos conozcan el objetivo establecido por la Dirección, las políticas, principios y normas adoptadas y su importancia para la seguridad de la Entidad, las responsabilidades generales y específicas en materia de seguridad de cada miembro de la empresa y otras referencias a documentación que puedan ser útiles.

La Dirección se compromete, además, a dotar al Comité de Seguridad de los medios y facultades necesarios para la realización de sus funciones.

3. Marco organizativo de la seguridad de la información

3.1 Comité: Funciones y Responsabilidades

Se recomienda la creación del Comité de Seguridad de la Información. Este típicamente coordina la seguridad de la información.

El Comité de Seguridad de la Información estará formado por:

- Responsable de la Información, Servicios y Seguridad
- Responsable del Sistema

En el ámbito del comité de seguridad, el Responsable de Seguridad tendrá como funciones:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad TIC reportará a la Dirección de OPENSERVICES y tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al Consejo.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de OPENSERVICES en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Consejo.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por OPENSERVICES y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de OPENSERVICES. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

3.2 Roles y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

Responsable de la Información y Servicios

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.

Responsable de Seguridad

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información.
- Además, ver 3.3.: Tareas.

Responsable del Sistema

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- Además, ver 3.3.: Tareas.

3.3 Tareas

RINFOSERV – Responsable de la Información y Servicio

RSEG – Responsable de la Seguridad

RSIS – Responsable del Sistema

Tarea	Responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFOSERV o el Comité de Seguridad de la Información
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	Elabora y aplica: RSEG
Implantación de las medidas de seguridad	RSEG
Aceptación del riesgo residual	RINFOSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: comité se seguridad aprueba : Consejo
Normativa de seguridad	elabora y aprueba: comité de seguridad de la información
Procedimientos operativos de seguridad	elabora y aprueba: RSEG aplica: RSIS
Estado de la seguridad del sistema	monitoriza: RSIS reporta: RSEG
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: comité de seguridad de la

	información
Planes de concienciación y formación	elabora: RSEG aprueba: comité de seguridad
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: comité de seguridad ejercicios: RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

3.4 Procedimiento de designación

El Responsable de Seguridad de la Información, Servicio y de Seguridad y el responsable de Sistema serán nombrados por el Consejo a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

3.5 Revisión de la Política de Seguridad de la Información

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Comité y difundida para que la conozcan todas las partes afectadas.

4. Datos de carácter personal

OPENSERVICES trata datos de carácter personal. El documento de seguridad, que se puede encontrar en la intranet, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de OPENSERVICES se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

5. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

6. Política de uso aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus

7. Seguridad de la gestión de los recursos humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información secreta.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

8. Seguridad física y del entorno

Para que una seguridad lógica sea efectiva es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.

8.1 Áreas seguras

OPENSERVICES tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las instalaciones de OPENSERVICES cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.

Los lugares donde se ubican los servidores y el cableado estarán en lugares aislados y sólo tendrán acceso las personas autorizadas y los proveedores de servicios cuando vayan acompañados por alguien autorizado.

Las ventanas y puertas deberán permanecer cerradas cuando las instalaciones estén vacías.

Se prohíbe expresamente al personal comer y beber cerca de los servidores y equipos informáticos. Así mismo, se tendrá especial cuidado con el manejo de cualquier producto que pueda verterse sobre activos de información.

Para la prevención de fugas de agua e inundaciones será necesaria la revisión periódica de la grifería, sanitarios y demás instalaciones que puedan causar daños de este tipo.

8.2 Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos críticos de OPENSERVICES estarán protegidos contra posibles fallos de energía u otras anomalías eléctricas, para ello se han instalado equipos de alimentación ininterrumpida.

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

La eliminación de equipos sólo se llevará a cabo por el Responsable de Seguridad o personal en el que éste delegue.

9. Gestión de comunicaciones y operaciones

9.1 Procedimientos operativos y responsabilidades

OPENSERVICES controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre su red y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red de OPENSERVICES existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del sistema. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

9.2 Protección frente a código malicioso y código móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de OPENSERVICES.

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el Responsable de Seguridad y autorizado por el Comité.

El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

9.3 Copias de seguridad

Los datos deben ser guardados en los servidores para asegurar que se realizan copias de seguridad habitualmente. Si la información se guarda en el disco duro de un PC, el usuario asignado a dicho PC es el responsable de realizar las copias de seguridad.

Habrá procedimientos para la realización de copias de seguridad que se archivarán para recuperar los datos en caso de incidencia. Estas copias estarán claramente identificadas y se guardarán en sitio seguro, preferiblemente fuera de las instalaciones de la organización.

También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

Si se corrompe la información en operación, hay que comprobar el software, el hardware y las comunicaciones implicadas antes de utilizar las copias de seguridad, para asegurarse de que no se pueda corromper la información contenida en ellas también.

9.4 Gestión de la seguridad de la red

Los elementos de red (switch, router...) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

9.5 Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

Los soportes (tanto papel como lógicos) que contengan información sensible deben permanecer en cajones o armarios cerrados bajo llave. Cuando alguna persona autorizada deba utilizarla para realizar alguna gestión relacionada con las labores propias de OPENSERVICES, ésta se hará responsable del buen cuidado de los soportes. No los dejará encima de su mesa cuando abandone su puesto de trabajo ni los colocará en cualquier otro lugar donde una persona sin autorización pueda verlos o apropiarse de ellos.

Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas.

Siempre será necesario registrar la eliminación de soportes que contengan información sensible para mantener una pista de auditoría.

9.6 Intercambio de información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

9.7 Seguimiento

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario.

10. Control de accesos

10.1 Requisitos del servicio para el control de accesos

La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto del área y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

En el caso de que visitantes o personal no autorizado acceda a las instalaciones o a la información de OPENSERVICES, estos deberán ir siempre acompañados por un miembro responsable de la Organización que controlará en todo momento que la seguridad de los recursos está garantizada.

10.2 Gestión de accesos de los usuarios

El administrador del sistema es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a Información y sistemas que no le son necesarios para las competencias de su trabajo.

10.3 Responsabilidades del usuario

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

De igual forma, es necesario configurar los equipos informáticos para que éstos queden bloqueados cuando el usuario no se encuentra en su puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el terminal.

También deben protegerse los puntos de entrada y salida de correo, las máquinas de fax y las impresoras que no se encuentren atendidas por alguna persona de Openservices.

10.4 Control de acceso a red

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con Openservices para mantener el mismo nivel de seguridad que si fueran empleados de la propia organización.

El Área de Informática controlará las altas y bajas de todos los usuarios.

11. Informática móvil y teletrabajo

En OPENSERVICES está permitido el teletrabajo previa validación de la solicitud pertinente. Antes de usar cualquier información hay que asegurarse de que el equipo en el que va a ser tratada está libre de virus o código malicioso.

Así mismo se permite el acceso a aplicaciones de forma remota, estando estas debidamente protegidas.

Cuando los equipos o la información propiedad OPENSERVICES están fuera de las instalaciones, el empleado que los está utilizando es el responsable de su seguridad y debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

12. Gestión de incidencias

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

13. Continuidad del servicio

Es imprescindible para OPENSERVICES establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, OPENSERVICES dispondrá de planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del servicio se incorporará a los procesos de OPENSERVICES y será responsabilidad de una o varias personas dentro de la entidad.

14. Obligaciones del personal

Todos los miembros de OPENSERVICES tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se realizarán periódicamente acciones de concienciación y sensibilización en materia de seguridad de la información que afecte a todos los miembros de OPENSERVICES. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

15. Terceras partes

Cuando Openservices preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando OPENSERVICES utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

16. Modificaciones respecto a la revisión anterior

Elaborado por: Start Up	Fecha: 19/09/2019
Revisado y Aprobado por: Comité de Seguridad	Fecha: 08/01/2024

EDICIÓN	FECHA	MODIFICACIONES
1	07/08/17	Primera Emisión
2		Revisión, actualizada legislación
3	19/09/2019	Revisión
4	08/01/2024	Revisión y actualización