índice

EDICIÓN	MODIFICACIONES	FECHA
1	Elaboración inicial Política	25-01-2019

1. INTRODUCCIÓN

Entre las responsabilidades asumidas por la Empresa Municipal de Servicios de Adeje S.A. (en adelante la Empresa), una de las más importantes es la de corresponder a la confianza que el Ayuntamiento de Adeje muestra hacia nuestra gestión en base a los distintos encargos de gestión que concierta con la empresa.
En este contexto, la confidencialidad, la disponibilidad y la integridad de la información que manejamos y gestionamos adquieren una especial relevancia.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la Empresa. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

La dirección de La Empresa, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento

2. OBJETIVO

El objetivo de la Política de Seguridad de la Información es asegurar la protección de la disponibilidad, integridad y confidencialidad de la información y de los sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

3. ÁMBITO DE APLICACIÓN

La presente Política de Seguridad de la Información se aplica a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de La Empresa. El personal sujeto a esta política incluye a todas las personas con acceso a la información, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de la Empresa.

El contenido de la Política de Seguridad de la Información, cuando así se requiera, será desarrollado en normas y procedimientos complementarios de seguridad.

4. ALCANCE DEL SISTEMA DE GESTIÓN SGSI

El alcance del sistema de gestión de seguridad de la información de la Empresa son los sistemas de información que dan soporte al almacenamiento y tratamiento de la gestión administrativa de los encargos de gestión del Ayuntamiento de Adeje.

5. PRINCIPIOS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción hasta su procesamiento, comunicación, transporte, almacenamiento, difusión y su eventual borrado o destrucción.
- La confidencialidad de la información debe garantizarse de forma permanente, evitando el acceso y la difusión a toda persona o sistema no autorizado.
- La integridad de la información debe ser asegurada, evitando la manipulación, alteración o borrado accidentales o no autorizados.
- La disponibilidad de la información debe salvaguardarse de forma que los usuarios y sistemas que lo requieran puedan acceder a la misma de forma adecuada para el cumplimiento de sus tareas y siempre que ello sea necesario.
- Se establecerán planes de continuidad para garantizar la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas y medios para su tratamiento.
- La Política de Seguridad de la Información es aprobada por la Dirección de La Empresa y su contenido y el de las normas y procedimientos que la desarrollan es de obligado cumplimiento.
- Todos los usuarios con acceso a la información tratada, gestionada o propiedad de La Empresa tienen la obligación y el deber de custodiarla y protegerla.
- La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas como UNE/ISO/IEC 27001.
- Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad (SOA) y la Empresa deberá establecer una planificación para su implantación y gestión.
- Las medidas de seguridad y los controles establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.

- Los usuarios que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con la empresa y con la legislación vigente y aplicable.

6. CLASIFICACIÓN DE LA INFORMACIÓN

La información se clasificará de acuerdo con la sensibilidad requerida en su tratamiento y a los niveles de seguridad y protección exigibles:

- Información Confidencial: Toda información especialmente sensible o que requiere un alto nivel de protección. Se deberán establecer medidas específicas de seguridad y de control para proteger la confidencialidad y la integridad de este tipo de información.

- Información de Uso Interno: Engloba la información menos sensible pero que es de uso exclusivamente interno en la empresa.

- Información Pública: Esta categoría engloba la información que ha sido autorizada para difundirse públicamente por la dirección de la empresa.

7. ROLES, RESPONSABILIDADES Y DEBERES

7.1. Usuarios

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de la empresa se considerará un usuario. Los usuarios son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos de la empresa. A cada usuario se le asigna uno o varios identificadores o credenciales personales únicos e intransferibles que deberá custodiar, evitando su uso por terceros. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Cumplir la Política de Seguridad de la Información y las normas, procedimientos e instrucciones complementarias.

- Proteger y custodiar la información de la empresa, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.

- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y las medidas de seguridad, con especial atención a las

requeridas por la Ley Orgánica de Protección de Datos y Derechos y Garantías Digitales (LOPDDGD).

7.2. Técnicos de tecnologías de la información

Los administradores de los sistemas de información y, en general, todos los técnicos relacionados con las tecnologías de la información deberán velar por la seguridad de los equipos, dispositivos, aplicaciones, entornos y sistemas que gestionan, además de proponer e implantar mejoras, mantener los sistemas protegidos y actualizados y cumplir las normas, procedimientos e instrucciones aprobadas por la Dirección.

En el diseño, instalación y gestión de los sistemas de información se deberá tener en cuenta la legislación aplicable y los controles de la norma UNE/ISO/IEC 27001 que procedan según el documento de aplicabilidad (SOA) aprobado por la Dirección de La Empresa

7.3. Responsable de Seguridad de la Información

Se designará un responsable de seguridad de la información que tendrá las siguientes funciones:

- Gestionar las políticas, normas y procedimientos de seguridad de la información.
- Controlar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.
- Gestionar las incidencias de seguridad.
- Administrar los riesgos relacionados con la seguridad de la información.
- Elaboración y mantenimiento de los planes de continuidad.
- Gestionar y supervisar el cumplimiento de la legislación vigente en materia de seguridad de la información (LOPD).
- Promover planes de formación, divulgación y concienciación en materia de seguridad de la información en la organización.

7.4. Dirección

La dirección de La Empresa está profundamente comprometida con la política descrita en este documento y es consciente del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

La dirección asume las siguientes responsabilidades:

- Aprobar y comunicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.

- Fomentar una cultura corporativa de seguridad de la información.

- Apoyar la mejora continua de los procesos de seguridad de la información.

- Asegurar la disponibilidad de los recursos necesarios para el sistema de gestión de seguridad de la información,

- Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos y asegurar la evaluación de estos al menos con una periodicidad anual.

- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.

- Evidenciar con las responsabilidades anteriores su liderazgo con respecto al sistema de gestión de la seguridad de la información y su compromiso con el cumplimiento de los requisitos aplicables a éste.

8. CONTRATACIÓN Y ADQUISICIONES

Todas las contrataciones y adquisiciones que supongan o requieran acceso o tratamiento de información clasificada como confidencial o de uso interno, deberán realizarse amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de información.

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberían tener en cuenta los siguientes requisitos:

Contratos: los proveedores deben tener un contrato escrito (o cualquier otro tipo de acto legal) con los responsables donde se detalle la duración, la naturaleza y el objeto del tratamiento, el tipo y las categorías de datos personales, así como las obligaciones y los derechos del responsable del tratamiento.

Seguridad de los datos: los proveedores deberán garantizar la implantación de las medidas de seguridad suficientes y las señaladas por el contratista, a fin de que se establezca un marco de seguridad adecuado.

Control por parte de las autoridades: los encargados de tratamiento podrán estar sujetos al control por parte de las autoridades de protección de datos (nacionales o europeas) en tanto son responsables de la gestión de datos personales.

Brechas de seguridad: tendrán la obligación de informar al contratante y al usuario, si es el caso, de las brechas de seguridad que hayan podido sufrir, dentro del plazo legalmente establecido de 72 horas.

Transferencias internacionales de datos: si el tratamiento de los datos o parte del mismo se va a llevar a cabo por parte del proveedor, fuera del ámbito de la UE, tendrá la obligación de informar del hecho al contratante y reflejarlo en el contrato que les vincule.

Privacy by default: cualquier tratamiento de datos deberá llevarse a cabo mediante la premisa de Privacy by default, es decir, teniendo en cuenta desde el momento mismo del diseño del tratamiento, los aspectos relacionados con la privacidad. Por tanto, el contratante deberá tener en cuenta lo previsto en la normativa relacionada con la privacidad, lo previsto en cuanto la seguridad que los proveedores le puedan ofrecer, valorando bajo su propia responsabilidad, el proveedor más adecuado.

Las empresas y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información confidencial o de uso interno, deberán conocer la Política de Seguridad de la Información y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las empresas y personas externas que accedan a la información de La Empresa deberán considerar dicha información, por defecto, como confidencial. La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

9. CONCIENCIACIÓN, DIVULGACIÓN Y FORMACIÓN

La presente Política de Seguridad de la Información debe ser conocida por todos los usuarios internos, externos e invitados y por las empresas que accedan, gestionen o traten datos de la Empresa.

Las normas y procedimientos complementarios a la Política de Seguridad de la Información también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas.

Se definirán, periódicamente, programas de comunicación, concienciación y formación y se entregará copia de la normativa correspondiente a los usuarios.

10. RESPUESTA A INCIDENTES DE SEGURIDAD

Cualquier compromiso de la confidencialidad, integridad o disponibilidad de la información de la empresa se considera un incidente de seguridad. Esto incluye, entre otros, el acceso, la eliminación, la destrucción, la modificación o la interrupción de la disponibilidad no autorizadas.

También se consideran incidentes de seguridad los meros intentos de compromiso de las condiciones anteriores, los de evitar, alterar o modificar las medidas de seguridad o las

violaciones o incumplimientos de la Política de Seguridad de la Información o de las normas y procedimientos complementarios.

Los usuarios son responsables de informar, de forma inmediata, de cualquier incidente de seguridad, o sospecha de este, al Responsable de Seguridad a través de los canales definidos en la organización para la comunicación de incidencias.