3 POLÍTICAS DE SEGURIDAD

3.1 PROPÓSITO

Las **Políticas de Seguridad** son documentos de alto nivel. Representan la filosofía y el talante del ASJ, en materia de seguridad. Es necesario, además, que las Políticas de Seguridad sean actualizadas periódicamente para que reflejen la realidad tecnológica y los cambios significativos en los procesos de seguridad de la Corporación Local.

Las Políticas de Seguridad tienen, como principal objetivo, evitar, reducir, eliminar y /o transferir los riesgos asociados a los SSII del ASJ. Por tanto, a continuación se describen las líneas fundamentales aprobadas por el ASJ para que el personal realice sus funciones y obligaciones garantizando la confidencialidad, integridad y disponibilidad de la información.

Las Políticas de Seguridad reflejan, además, los requerimientos legales y éticos de todas las funciones del personal del ASJ, respecto a su operativa habitual.

Con dicho propósito, el presente documento, contempla lo establecido en la LOPD, así como los requisitos exigidos mediante el Real Decreto 994/1999, de 11 de Junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (en adelante, Reglamento), la norma ISO 17799.

3.2 ÁMBITO DE APLICACIÓN

3.2.1 Perspectiva Institucional

Serán de aplicación al conjunto de ficheros con DCP y SSII del ASJ que como organismo autónomo con personalidad jurídica propia y

plena capacidad de obrar, ostenta la identidad de Responsable de Tratamiento/ficheros en los términos del Art. 3 d) de la LOPD.

3.2.2 Perspectiva Material

Se aplicarán a todos los recursos informáticos del ASJ que traten DCP de su titularidad; esto incluye, pero no se limita a:

- *red interna (LAN)*
- *equipos y elementos de interconexión (electrónica de red)*
- *servidores Internet*
- *servidores que contengan bases de datos*
- *otros servidores*
- *terminales*
- *ordenadores personales*
- *sistemas de impresión de cualquier tipo*
- *ordenadores portátiles*
- *sistemas de grabación de datos de cualquier tipo*
- *información contenida en cualquiera de los sistemas anteriores*

3.2.3 Perspectiva Personal

Estas Políticas son de obligado cumplimiento para todo el personal del ASJ.

Las políticas, normativas y procedimientos internos contenidos en el presente documento deberán ser puestos en conocimiento de todo el personal del ASJ, **con el objeto de dar debido cumplimiento a la obligación contenida en el Art. 9.2 del Reglamento**.

3.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

3.3.1 Confidencialidad y deber de secreto

Se debe proteger la información confidencial, estableciendo controles para su envío al exterior mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.

Los usuarios de los SSII del ASJ deberán guardar, en todo caso, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación con el ASJ. **Esta obligación continuará vigente tras la extinción del contrato de trabajo.**

Ningún colaborador en proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada al ASJ.

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, un empleado de una empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión se produce por motivos profesionales autorizados, y es estrictamente temporal, con obligación de secreto, y sin que por ello se le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

Asimismo, deberán ser devueltos la documentación y/o soportes mencionados, después de la finalización de las tareas que han originado dicha posesión. **La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y**

sin conocimiento de ASJ no supondrá, en ningún caso, una infracción del ASJ de este punto.

El incumplimiento de estas obligaciones de confidencialidad y deber de secreto, puede constituir un delito de revelación de secretos, previsto en el artículo 197 del Código Penal.

3.3.2 Propiedad Intelectual

El ASJ se compromete a utilizar exclusivamente software autorizado en sus SSII. Está prohibido expresamente al personal operar con software procedente de cualquier otra fuente no autorizada.

El ASJ se compromete de igual forma a utilizar únicamente software con licencia y no aceptar el empleo de más copias de las autorizadas según la licencia.

Para el desarrollo interno de software, éste sólo deberá contener las funcionalidades especificadas en los análisis y no otras con finalidades distintas o fraudulentas.

3.3.3 Seguridad Física

El ASJ establece la necesidad de planificar la localización física de los SSII teniendo en cuenta la seguridad de los mismos, a tal efecto almacenará los soportes de los SSII en una ubicación segura con acceso restringido.

Es preciso evaluar y prevenir riesgos potenciales de incendios, catástrofes naturales y otro tipo de riesgos. El análisis de la seguridad física no quedará limitado al emplazamiento de los SSII, sino que tendrá en cuenta los peligros del vecindario. El entorno de trabajo debe

mantener las condiciones que satisfagan continuamente las normas de seguridad física y no permitan deterioros.

3.3.4 Acceso Físico

Las Áreas sensibles del ASJ deben ser protegidas con los mecanismos adecuados. Solamente el personal autorizado tendrá acceso a las Áreas sensibles. Se definirán normativas y procedimientos para controlar el acceso del personal interno y externo. Todo el material confidencial se almacenará con las debidas medidas de seguridad, incluso cuando se localicen en áreas seguras y estando disponibles solamente para el personal autorizado.

3.3.5 Identificador de usuario y contraseña

Todos los usuarios con acceso a un sistema de información, dispondrán de una única autorización de acceso compuesta por identificador de usuario y mecanismo de autenticación basado en contraseña.

Ningún usuario recibirá un identificador de acceso a Recursos Informáticos o Aplicaciones hasta que no acepte formalmente el Documento de Política de Seguridad vigente.

Los usuarios tendrán acceso autorizado exclusivamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por cada Responsable de Autorización de Accesos.

El ASJ definirá una longitud mínima de las contraseñas y estarán constituidas por una combinación de caracteres alfabéticos y numéricos. Los identificadores temporales se

configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

3.3.6 Incidencias

Es obligación de todo el personal que accede a los SSII del ASJ comunicar cualquier incidencia que se produzca en los mismos o en cualquier otro recurso informático.

El ASJ se compromete a mantener un **Registro de Incidencias de Seguridad** en el que se almacene y revise toda la información relativa a los posibles acontecimientos que sucedan en sus SSII y, en concreto, aquellas que puedan afectar a la seguridad de los DCP.

3.3.7 Conformidad Legal

El ASJ se compromete a poner los medios necesarios para **cumplir con cualquier normativa u obligación contractual relacionada con la seguridad de la información** para mejor protección de sus intereses.

Todos los requisitos legales, reglamentarios y contractuales serán explícitamente definidos y documentados para cada uno de los SSII. Igualmente, se especificarán los controles y responsabilidades individuales para cumplir con dichos requisitos.

3.3.8 Uso apropiado de los recursos

Los recursos de los SSII están disponibles exclusivamente para el cumplimiento de las funciones y obligaciones de cada puesto de trabajo y propósito de la operativa para la que fueron diseñados e implantados. **Todo el personal usuario de dichos**

recursos, debe saber que puede ser fiscalizado en el correcto uso de estos medios.

Cualquier Fichero introducido en la red interna (LAN) o en el puesto de trabajo del Usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a Propiedad Intelectual y protección de DCP.

3.3.9 Copia de Seguridad

Todos los datos almacenados en los SSII del ASJ deben estar protegidos frente a pérdida o daños, mediante la aplicación de procedimientos eficaces de copias de seguridad. Estos procedimientos se llevarán a cabo con la frecuencia adecuada para garantizar que la Corporación Local no sufra interrupciones, debidas a fallos de los sistemas.

Si se generan o almacenan datos en los ordenadores personales, será responsabilidad de cada usuario garantizar la periodicidad de las copias de seguridad.

3.3.10 Plan de Contingencias

El ASJ mantendrá un Plan de recuperación de información, ante desastres y/o catástrofes que comprenderá todos los SSII críticos de la Corporación Local (en concreto los ficheros con DCP). El plan especificará las acciones a emprender en caso de que todos o parte de los servicios de los SSII queden interrumpidos temporal o definitivamente.

Éste deberá basarse en un análisis de riesgos de las amenazas potenciales que se puedan presentar y de los medios disponibles para

continuar operando. Es preciso articular procedimientos de recuperación de datos para abordar a distintos niveles las incidencias que puedan presentarse.

3.3.11 Herramientas de cifrado

Las redes internas y externas no están generalmente protegidas contra posibles intrusiones de terceros. En estos casos, si la información tiene que ser protegida, los usuarios deberán aplicar las herramientas de cifrado autorizadas. Igualmente, las video conferencias no incluirán asuntos sensibles a menos que se activen las herramientas de cifrado disponibles.

Siempre que se envíe información confidencial a través de redes públicas, como Internet, se deberán utilizar las herramientas de cifrado aprobadas. Siempre se almacene información secreta en los ordenadores, se realizará utilizando herramientas de cifrado.

Muchas de las rutinas para el cifrado exigen que el usuario provea o introduzca un código, frase etc... Los usuarios deben proteger su confidencialidad con especial diligencia, igual que con las contraseñas para evitar su difusión no autorizada.

3.3.12 Impresión, copiado y reparación de máquinas reprográficas

Si una impresora, fotocopiadora, fax o cualquier otro dispositivo de salida de documentación con información confidencial se estropea o paraliza, el usuario afectado no debe abandonar la máquina hasta que se reanude el proceso o se deseche tal información. **Todas las copias de material sensible deben desecharse apropiadamente utilizando las herramientas aprobadas por el ASJ**.

No debe enviarse información sensible mediante fax a menos que el personal autorizado, y esté presente en el momento del envío (a su vez personal autorizado debe estar presente en la recepción), para manejar los documentos apropiadamente. No deben enviarse faxes con información sensible a través de terceros intermediarios ajenos al ASJ, sin autorización expresa. La información sensible sólo puede enviarse mediante fax si la conexión está protegida con sistemas de cifrado aprobados. La recepción de información sensible por fax, debe confirmarse inmediatamente. Todos los faxes deben emplear una página de presentación.

Cuando se vayan a imprimir documentos con información sensible, los usuarios deben estar presentes para prevenir el descubrimiento por parte de terceros no autorizados o imprimir mediante impresoras localizadas en áreas seguras o que estén bajo el control del personal autorizado.

La reparación de faxes, impresoras y otros dispositivos de copias debe ser realizada por proveedores que hayan firmado los acuerdos de Confidencialidad con el ASJ.

3.3.13 Ordenadores portátiles y Teletrabajo

Todos los ordenadores portátiles que están bajo el control del ASJ y se utilicen para procesar información de la Corporación Local, deben estar protegidos con una herramienta de control de acceso aprobada. Estos controles de acceso deben prevenir el uso indebido de los equipos y el acceso indebido a la información.

La información sensible no debe salir de los locales del ASJ. Si hiciese falta trasladar información sensible fuera de las oficinas, se

protegerá con las herramientas de cifrado aprobadas. Igualmente, si se transmite información a través de redes públicas, las comunicaciones se protegerán con las herramientas de cifrado aprobadas. Todos los dispositivos portátiles y remotos que almacenen información sensible deben, utilizar además herramientas de cifrado del disco duro.

El acceso remoto a los SSII del ASJ, requieren que todos los usuarios se autentiquen mediante sistemas de identificación aprobados. Las conexiones entrantes a los SSII a través de un módem o VPN se prohíben a menos que exista aprobación específica.

Los usuarios no deben almacenar contraseñas, identificadores de usuario o cualquier otra información de acceso, en sistemas portátiles o remotos. Si se utilizan generadores de contraseñas dinámicos u otros mecanismos de control de acceso, estos no deben almacenarse en la misma bolsa que los ordenadores portátiles.

Los usuarios deben tener cuidado de no discutir acerca de información sensible del ASJ en lugares públicos como en hoteles, restaurantes y ascensores. El visionado de información sensible en una pantalla o la lectura de documentos en lugares públicos. Los usuarios deben tener cuidado para no proporcionar información sensible en mensajes de correo o de móvil.