3) Jefatura de personal

Esta función podrá ser desarrollada por la Secretaría de Organización.

Sus funciones serán

a. Adecuar el cumplimiento de las actuaciones laborales a la legislación y a los acuerdos alcanzados con la representación legal de los trabajadores y las trabajadoras.

b. Dirigir la interlocución con los órganos de representación laboral.

c. Implementar la política salarial de la organización.

d. Representar al partido a todos los efectos laborales.

e. Llevar a cabo las funciones disciplinarias y todas aquellas propias de su competencia.

9. Medidas de seguridad de la información y Equipo de Infraestructura Tecnológica

La información es uno de los activos más valiosos de cualquier organización y de ella depende buena parte del éxito de su funcionamiento.

Por ello resulta prioritario asegurar la integridad, la confidencialidad y la disponibilidad de la información.

La implantación de las nuevas tecnologías de la información ha incrementado el riesgo de las organizaciones frente al acceso de personas no autorizadas a la información confidencial. En este sentido, y concretamente en Iniciativa del Pueblo Andaluz, casi la totalidad de la información se almacena en equipos informáticos, dispositivos móviles, soportes de almacenamiento y redes de comunicación de datos, los cuales están sometidos permanentemente a las amenazas de destrucción o sustracción, tanto desde dentro de la propio partido como desde el exterior.

Los riesgos pueden ser físicos (averías, incendios, inundaciones, terremotos, vandalismo…) o informáticos (hackers, suplantación de identidad, spam, virus, sustracción de información, espionaje…), y estas situaciones pueden afectar a la integridad, la confidencialidad o la disponibilidad de nuestra información y de nuestros recursos informáticos, lo que haría inviable la continuidad del trabajo.

Por tanto, para proteger nuestra organización de todas estas amenazas es imprescindible establecer los protocolos adecuados e implementar los controles de seguridad necesarios en función del riesgo y de la eficacia de las medidas que deban adoptarse.

9.1. Sistema de Gestión de la Seguridad de la Información (SGSI)

Uno de los objetivos de Iniciativa del Pueblo Andaluz a medio plazo es el establecimiento de un Sistema de Gestión de la Seguridad de la Información, basado en **la norma UNE-ISO/IEC 27001**, con el fin de fijar las políticas, los procedimientos y los controles que permitan reducir los riesgos y garantizar la integridad, la confidencialidad y la disponibilidad de nuestra información y de nuestros recursos informáticos.

9.2. Documento de Seguridad de Protección de Datos

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que el responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Igualmente se establece legalmente que las medidas de índole técnica y organizativa que los responsables de los tratamientos o de los ficheros, así como los trabajadores que se encargan de ello, han de implantar para garantizar la seguridad en lo relativo a los ficheros, centros de tratamiento, locales, equipos, sistemas, programas y a las personas que intervengan en el tratamiento de datos de carácter personal.

Entre estas medidas se encuentra la elaboración de un documento que recogerá las disposiciones de índole técnica y organizativa acordes a la normativa de seguridad vigente que será, por tanto, de obligado cumplimiento para quienes tengan acceso a los datos de carácter personal.

En consonancia con dichas disposiciones legales se ha elaborado un Documento de Seguridad aplicable a los ficheros que se encuentran bajo la responsabilidad de Iniciativa del Pueblo Andaluz y que contienen datos de carácter personal (incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal), y que deben ser protegidos de acuerdo con lo dispuesto en normativa vigente, así como las personas que intervienen en el tratamiento de dichos datos y los locales en los que se ubican.

Todas las personas que tengan acceso a los datos de los ficheros de Iniciativa del Pueblo Andaluz, a través del sistema informático habilitado para acceder a ellos o a través de cualquier otro medio automatizado de acceso a los ficheros, se encuentran obligadas por ley a cumplir lo establecido en el Documento de Seguridad y están, por tanto, sujetas a las consecuencias que pudieran derivarse en caso de incumplimiento.

9.3. Protocolos de Seguridad de la Información

9.3.1. Incidencias de seguridad

Se considera una «incidencia de seguridad» cualquier incumplimiento de la normativa desarrollada en el Documento de Seguridad, así como cualquier anomalía o situación de riesgo que afecte o pueda afectar a la seguridad, la integridad, la confidencialidad y la disponibilidad de los datos de carácter personal, a la información confidencial o a los recursos informáticos de Iniciativa del Pueblo Andaluz.

Cualquier miembro de Iniciativa del Pueblo Andaluz que tenga conocimiento de una incidencia relativa a la seguridad está obligado a notificarla de manera urgente al Delegado de Protección de Datos para que este proceda a activar el protocolo de seguridad correspondiente. En caso contrario, es decir, si se no se notifica una incidencia de seguridad que algún miembro del partido conoce,

este hecho será considerado como una falta grave contra la seguridad de la información de Iniciativa del Pueblo Andaluz.

9.3.2. Ejemplos de incidencias de seguridad y situaciones de riesgo

a. El bloqueo de acceso a usuarios autorizados por riesgo de destrucción de datos o alteración de sistemas.

b. El cambio urgente de contraseñas de acceso a sistemas y accesos como medida de prevención.

c. Las modificaciones / accesos no autorizados de información.

d. La no revisión o modificación del Documento de Seguridad cuando ello fuera preciso.

e. La pérdida de información.

f. Las copias indebidas de datos en los puestos de trabajo.

g. El mal funcionamiento durante la realización de copias de seguridad.

h. Los errores del sistema o en las transacciones o en la base de datos.

i. Los accesos no autorizados a las salas donde se ubiquen los sistemas y soportes informáticos (CPD, oficina, caja de seguridad, etcétera).

j. La caída del sistema informático.

k. El intento no autorizado de salida de soportes.

l. La destrucción total o parcial de soportes físicos.

m. El conocimiento por parte de terceros del identificador de usuario y de la contraseña.

n. La existencia de sistemas sin las debidas medidas de seguridad.

o. El cambio de ubicación física de los ficheros.

p. La no realización de las copias de respaldo preceptivas en el tiempo que se fija en el Documento de Seguridad.

q. La carencia de los controles periódicos que deben ser efectuados.

r. La omisión de registro en la entrada o salida de los soportes, o bien la falta de constancia de los datos que deban ser registrados.

s. El incumplimiento de las medidas establecidas para el desecho o la reutilización de los soportes.

t. La falta de autorización por escrito del responsable del fichero para poder ejecutar la recuperación de los datos.

u. La distribución en soportes, o la transmisión por redes de telecomunicación, de información sensible o susceptible de ser manipulada.

v. La omisión de alguno o de todos los datos que deben figurar en el registro de acceso.

w. La eliminación de los datos del registro de acceso antes del periodo de dos años.

x. La omisión de comprobaciones periódicas, en el tiempo establecido en el Documento de Seguridad.

9.3.3. Protocolos de Seguridad de la Información y continuidad de servicios críticos

En el Documento de Seguridad de Protección de Datos se detallan los diferentes protocolos de seguridad diseñados en función del tipo de incidencia, del riesgo de destrucción o sustracción de información y de la eficacia de las medidas que deban adoptarse.

Los protocolos tenderán a corregir las incidencias de seguridad y a reducir de forma urgente la destrucción o sustracción de los datos de carácter personal, de la información confidencial o de los recursos informáticos de Iniciativa del Pueblo Andaluz, garantizando la continuidad de los servicios informáticos de la organización.

Ante situaciones de riesgo inminente se aplicará de forma inmediata el Protocolo de bloqueo urgente de acceso a sistemas y servicios ante incidencias de seguridad y riesgo de destrucción o sustracción de datos previstos en el Documento de Seguridad.

9.4. Equipo de Infraestructura Tecnológica

El Equipo de Infraestructura Tecnológica estará conformado por el personal técnico que sea necesario para garantizar el cumplimiento de sus funciones como proveedor de infraestructura tecnológica a todas las áreas de Iniciativa del Pueblo Andaluz, y como responsable de la implantación de las medidas técnicas que garanticen la seguridad de la información y la protección de los datos personales.

Estará dirigido por la Secretaría de Organización, en colaboración con la Delegada o el Delegado de Protección de Datos y el Responsable de Seguridad Informática, y entre sus áreas funcionales se encontrarán al menos las siguientes:

a. Sistemas. Esta área se encargará de asegurar el correcto funcionamiento de la infraestructura tecnológica y de la implantación y mantenimiento de las medidas y sistemas técnicos y organizativos necesarios para garantizar, a su vez, la seguridad de la infraestructura tecnológica y el cumplimiento de las medidas de seguridad establecidas en el Documento de Seguridad.

b. Desarrollo. Esta será el área encargada de las aplicaciones, las bases de datos, las páginas web y los formularios online.

c. Soporte. Esta área se encargará de dar soporte informático a las diferentes áreas del partido, y del mantenimiento de los equipos y los dispositivos.