POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 13/12/2021 por la Dirección.
Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

Sociedad de Agricultores de la Vega (SAV) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada o los servicios prestados.

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 de forma rápida y eficiente frente a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar 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.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de 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 y en la solicitud de ofertas.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1 PREVENCIÓN

Los departamentos deben 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 los departamentos deben implementar 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, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, los departamentos deben:

- 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.

2.2. 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.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

• Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de y a todos los miembros de la organización, sin excepciones y el alcance de esta es: "Procesos para la protección de la información que dan soporte a los servicios de limpieza, recogida, jardinería, cementerios y depuración de aguas."

4. MISIÓN

SAV es una empresa de servicios fundada en 1900, que desarrolla su actividad en el ámbito del Medio Ambiente, desde la limpieza de espacios públicos y privados y la gestión integral de los residuos hasta el mantenimiento de instalaciones depuradoras de aguas. Actualmente presta sus servicios en la Comunidad Autónoma de Valencia, Cataluña, La Rioja, Castilla la Mancha, Andalucía, Aragón, Navarra, País Vasco, Murcia, Galicia, Asturias, Extremadura, Baleares y Madrid.

5. MARCO NORMATIVO

SAV se encuentra a la normativa indicada en el Anexo I. Este Anexo se irá actualizando en función de nuevas normativas que sean de aplicación a SAV.

Objetivos:

La gestión de la seguridad de la información apoya la consecución de los siguientes objetivos alineados con nuestra actividad de negocio:

- Proveer todos los recursos, formación y acompañamiento necesarios para facilitar que todo su personal alcance una adecuada cultura de seguridad de la información.
- Ofrecer garantías de seguridad de la información a nuestros clientes y otras partes interesadas.
- Convertir la seguridad de la información en parte integral del trabajo, siendo reflejada en cada actividad que se realice, formando al

personal en nuestro SGSI, haciendo que se sientan responsables e involucrados con su trabajo mediante una comunicación fluida.

- Proteger los procesos críticos del negocio para lograr la continuidad ante posibles contingencias.
- Cumplir con la legislación vigente.

Para el logro de estos objetivos la Dirección de SAV, se compromete a aportar los recursos necesarios ya a trabajar junto con el comité de Seguridad de la Información en la mejora continua del Sistema de Gestión.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Gestión de la Seguridad de la Información estará formado por el Responsable del Servicio, el Responsable de la Información, el Responsable de Seguridad, el Responsable del Sistema de Gestión y el Responsable del Departamento de Informática. El Comité tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información en SAV.
- Elaborar la estrategia de evolución de SAV en lo que respecta a la 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
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por SAV y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. 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 de seguridad 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 SAV.
- 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.

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

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Los diferentes roles junto con sus respectivas funciones y responsabilidades, vienen descritos a continuación.

Responsable del Servicio

- 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.
- Aprobar formalmente el nivel de seguridad del servicio.

Responsable de la Información

- 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.
- Aprobar formalmente el nivel de seguridad de la información.
- Promover que el tratamiento de los datos personales efectuados por SAV, se efectúe de forma respetuosa con la normativa
- Desde el punto de vista de la seguridad y teniendo en cuenta el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables deberá velar por que se garantice una seguridad adecuada de los datos personales y determinar las medidas de seguridad concretas que tendrá que proponer al responsable del tratamiento.

Responsable de Seguridad

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
  Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Gestionar la monitorización del estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar la investigación de los incidentes de seguridad.

Responsable del Sistema de Gestión de la Información

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Responsable departamento de informática

- 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.

En el Anexo II se recogen los nombramientos de cada uno de los miembros del comité.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El cumplimiento de las responsabilidades definidas en esta Política de Seguridad está determinado por el acceso a los diferentes cargos que se vinculan a esas responsabilidades. Será competencia de la Dirección, designar a cada uno de los miembros del Comité, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Gestión de la Seguridad de la Información 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 mismo comité y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

SAV trata datos de carácter personal sometidos al RGPD Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de estos datos, así como a la LOPDyGDD, Ley Orgánica 3/2018 de protección de datos personales y garantía de derechos digitales.

El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de SAV 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.

El inventario de Registros de Actividades del Tratamiento RAT, recoge los ficheros y tratamientos de datos afectados, así como los responsables correspondientes. Todos los sistemas de información de SAV 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 RAT.

Las medidas técnicas y organizativas de seguridad están adaptándose al estado de la técnica, los costes de aplicación y la naturaleza, ámbito, objetivo,

contexto y finalidad del tratamiento, así como a riesgos de probabilidad e impacto variable de los derechos de las personas físicas.

8. GESTIÓN DE RIESGOS

SAV deberá realizar un análisis de riesgos de todos los sistemas, 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 Gestión de la Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Gestión de la Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. GESTIÓN DOCUMENTAL

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en los procedimientos: Procedimiento de Seguridad y Procedimiento Protección de la información, en el que queda definido que la información se clasifica en los siguientes tipos: Pública, interna y confidencial.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de SAV en diferentes materias:

Normativa Seguridad, Procedimientos de seguridad, Proceso de autorización.

Los documentos anteriores estarán a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

11. OBLIGACIONES DEL PERSONAL

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

Todos los miembros de SAV asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de SAV, 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.

12. TERCERAS PARTES

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

Cuando SAV utilice servicios de terceros o ceda información a terceros, se les hará partícipes 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.

La Dirección
S.A. Agricultores de la Vega

ANEXO I: Marco Normativo

Normativa del sector público

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se trasponen al ordenamiento jurídico española las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 2/2015, de 2 de abril, de la Generalitat, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones

Normativa relacionada con la Privacidad y la Seguridad

- Reglamento 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica.

- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Otra Normativa

- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley 18/2018, de 13 de julio de la Generalitat Valenciana, para el fomento de la responsabilidad social.
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Los distintos convenios colectivos que sean de aplicación.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

La Dirección

S.A. Agricultores de la Vega.

Rev2. 13/12/2021

ANEXO II: Nombramientos

Responsable del Servicio y Responsable de la Información.

Nombre y apellidos	JOSÉ ANTONIO CALVO ORTS
Departamento	JURÍDICO
Cargo	JURÍDICO

Responsable de la Seguridad

Nombre y apellidos	GUILLERMO SANCHO
Departamento	SISTEMAS INTEGRADOS DE GESTIÓN
Cargo	TÉCNICO DE SISTEMAS

Responsable Sistema de Gestión de la Información

Nombre y apellidos	CRISTINA GOZALBO LAGUARDA
Departamento	INFORMÁTICA
Cargo	INFORMÁTICA

Responsable Departamento Informático

Nombre y apellidos	EMILIO CHAPÍ
Departamento	INFORMÁTICA
Cargo	RESPONSABLE DEP. INFORMÁTICO