POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Política de Seguridad de la Información de CONESA GROUP, conforme a lo dispuesto en el 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 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

25/11/2025

INDICE:

1. INTRODUCCIÓN.

La Seguridad de la Información en CONESA GROUP se define como la preservación de la confidencialidad, integridad y disponibilidad de la información y de los activos que la sustentan. Este compromiso se extiende a los procesos, sistemas y personas que acceden o gestionan información crítica para el negocio.

La protección de la información es esencial para garantizar la continuidad del negocio, el cumplimiento normativo y la confianza de nuestros grupos de interés. La organización reconoce la importancia creciente de la ciberseguridad y la necesidad de una gestión proactiva frente a amenazas emergentes.

2. OBJETIVOS.

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.

2.1. Prevención. Todo el personal y servicios de CONESA GROUP 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 deben implementarse las medidas mínimas de seguridad determinadas conforme al análisis de riesgo preceptivo, incorporando herramientas actualizadas y procedimientos adaptados a nuevas amenazas tecnológicas.

2.2. Detección. Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, la operativa y los sistemas deben monitorizarse de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se reforzará la capacidad de detección mediante soluciones avanzadas de supervisión.

2.3. Respuesta. CONESA GROUP debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados.

- Establecer protocolos para el intercambio de información relacionada con el incidente.

Todo el personal deberá conocer y aplicar los procedimientos establecidos ante incidentes.

2.4. Recuperación. Para garantizar la disponibilidad de los servicios críticos, CONESA GROUP desarrollará y mantendrá planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación. Dichos planes deberán revisarse regularmente y ser objeto de pruebas para validar su eficacia.

3. MARCO NORMATIVO.

La presente política se alinea con la legislación vigente, incluyendo:

- Reglamento (UE) 2016/679 (RGPD).
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico.
- Recomendaciones de la Agencia Española de Protección de Datos y del CCN-CERT.

Además, se tendrán en cuenta guías sectoriales y requisitos contractuales específicos de clientes o reguladores, cuando apliquen

4. ORGANIZACIÓN DE LA SEGURIDAD.

4.1. Designación de responsables.

CONESA GROUP designará al Responsable de Seguridad de la Información y, en su caso, al Delegado de Protección de Datos. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

4.2. Responsable de seguridad.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas para verificar el cumplimiento de los requisitos del mismo.

- Gestionar o promover 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.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes.

5. DATOS DE CARÁCTER PERSONAL.

El tratamiento de datos personales se regirá por principios de minimización, licitud, exactitud y transparencia. Solo accederán a estos datos las personas autorizadas y formadas. Los sistemas se ajustarán a los niveles de seguridad establecidos por la normativa vigente.

CONESA GROUP no trata datos especialmente sensibles conforme a la normativa aplicable. No obstante, se mantendrán medidas técnicas y organizativas proporcionales al tipo de datos tratados, garantizando la protección frente a accesos no autorizados, pérdida o alteración.

Se promoverá la privacidad desde el diseño y por defecto en todos los procesos y sistemas que traten datos personales.

6. GESTIÓN DE RIESGOS.

Todos los activos de información serán sometidos a un análisis de riesgos que se actualizará:

- Anualmente.
- Ante cambios relevantes en sistemas o procesos.
- Tras la detección de vulnerabilidades o incidentes significativos.

Este análisis permitirá identificar amenazas potenciales, evaluar la probabilidad e impacto de los riesgos asociados, y priorizar la adopción de controles eficaces. La

metodología aplicada deberá ser coherente con estándares reconocidos y adaptarse a la naturaleza de los activos y procesos críticos.

Los resultados del análisis se documentarán formalmente y serán tenidos en cuenta en la planificación de medidas técnicas, organizativas y de continuidad operativa.

7. OBLIGACIONES DEL PERSONAL.

Todos los trabajadores de CONESA GROUP tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento, siendo responsabilidad de CONESA GROUP disponer los medios necesarios para que la información llegue a los afectados.

Todo empleado es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.

Todo empleado es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de los procedimientos de seguridad internos.

Se sancionará cualquier violación a esta política y a cualquier política o procedimiento de seguridad que se haya comunicado.

CONESA GROUP velará porque se brinde concientización y entrenamiento en materia de seguridad de la información a todo el personal.

8. TERCERAS PARTES.

Los terceros que accedan a sistemas o información de CONESA GROUP deberán:

- Firmar acuerdos de confidencialidad y cumplimiento.
- Alinear sus prácticas con esta política y someterse a controles cuando sea necesario.
- Informar de cualquier incidencia o vulnerabilidad detectada en los servicios prestados.

CONESA GROUP evaluará periódicamente los riesgos derivados de la relación con terceros y aplicará medidas de supervisión proporcionales al nivel de criticidad de los servicios contratados.

9. APROBACIÓN Y ENTRADA EN VIGOR.

Esta política entra en vigor tras su aprobación por la Dirección de CONESA GROUP y será revisada al menos cada dos años, o cuando se produzcan cambios relevantes en el entorno normativo, tecnológico o de negocio.

Las versiones anteriores quedarán sin efecto desde la fecha de entrada en vigor de la presente.

En Villafranco del Guadiana, a 25 de noviembre de 2025.

Fdo. Manuel Vázquez Calleja.

CEO