Noviembre 2025

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE LA PRIVACIDAD

La presente Política Corporativa de Seguridad de la Información y Gestión de la Privacidad de Datos Personales de Laboratorios NORMON, S.A. ("NORMON") expresa el compromiso del Consejo de Administración de NORMON junto con la Dirección General y el Comité de Seguridad de la Información de NORMON, de proteger la información y los datos personales que gestiona en el desarrollo de sus actividades. Esta Política es de aplicación a todas las áreas, ubicaciones, personas trabajadoras y partes interesadas de NORMON, y se fundamenta en los requisitos y buenas prácticas establecidos por las normas UNE-EN ISO/IEC 27001, UNE-EN ISO/IEC 27701, el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 3/2018 (LOPDGDD), el Esquema Nacional de Seguridad (ENS) y demás legislación y normativa sectorial aplicable.

1. Definición de la Seguridad de la Información: A efectos de esta política y conforme a la Norma UNE-EN ISO/IEC 27001, la seguridad de la información se entiende como la preservación de la confidencialidad (acceso solo por personas autorizadas), integridad (exactitud y completitud), disponibilidad (acceso cuando sea necesario), autenticidad (veracidad del origen) y trazabilidad (registro y seguimiento de las acciones sobre la información) de los activos de información. En el ámbito de la privacidad, según UNE-EN ISO/IEC 27701 y el RGPD, se amplía esta definición para incluir la protección de los derechos y libertades de las personas titulares de datos personales, asegurando un tratamiento lícito, leal y transparente.

2. Objetivos de Seguridad de la Información y Privacidad: El objetivo principal de NORMON es garantizar, de manera alineada con los objetivos estratégicos empresariales, la protección de sus activos de información y datos personales, asegurando la continuidad del negocio, la confianza de clientes, empleados y terceros, y el cumplimiento de los requisitos legales, normativos y contractuales. Para ello, se establece un marco para definir y revisar objetivos específicos de seguridad y privacidad, que se concretan anualmente y se alinean con los siguientes propósitos:
   - Proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
   - Salvaguardar los datos personales frente a cualquier riesgo de acceso, alteración, pérdida o destrucción no autorizados.
   - Garantizar la continuidad, resiliencia operativa y protección de los servicios críticos.
   - Promover la cultura de seguridad y privacidad en toda la organización.
   - Prevenir, detectar y responder eficazmente ante incidentes de seguridad y brechas de datos personales.
   - Evaluar y mejorar de manera continua el Sistema de Gestión de Seguridad de la Información y Privacidad (SGSI).

3. Marco Normativo: NORMON se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad de la información y protección de datos personales. Esto incluye, entre otros, el RGPD, la LOPDGDD, el ENS, la Directiva NIS2, así como los estándares UNE-EN ISO/IEC 27001 y 27701, y cualquier requerimiento derivado de acuerdos con clientes, proveedores o autoridades. Se garantiza que las políticas, procedimientos y controles internos están alineados con el marco normativo vigente y que se revisan periódicamente para mantener su adecuación.

4. Principios Generales: Las actuaciones en materia de seguridad de la información y gestión de la privacidad en NORMON se fundamentan en los siguientes principios:

- Confidencialidad: Garantizar que la información solo sea accesible por quienes estén debidamente autorizados.
- Integridad: Salvaguardar la exactitud y completitud de la información y sus métodos de tratamiento.
- Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran.
- Autenticidad: Verificar y asegurar la identidad de los usuarios, sistemas y procesos, así como la veracidad del origen de la información.
- Trazabilidad: Registrar y poder seguir todas las acciones realizadas sobre la información, permitiendo su seguimiento y auditoría.
- Legalidad y Transparencia: Cumplir con la normativa aplicable y asegurar la transparencia en el tratamiento de datos personales.
- Minimización de datos: Limitar el tratamiento de datos personales a lo estrictamente necesario para los fines declarados.
- Responsabilidad Proactiva: Demostrar la aplicación efectiva de medidas técnicas y organizativas apropiadas.
- Gestión de Riesgos: Identificar, evaluar y tratar los riesgos que puedan afectar a la seguridad de la información y la privacidad.
- Mejora Continua: Revisar y perfeccionar de manera sistemática el sistema de gestión.
- Concienciación y Formación: Promover el conocimiento y la implicación de toda la plantilla y terceros en materia de seguridad y privacidad.

5. **Compromiso con la Gestión de Evaluaciones de Riesgos, RATs y EIPDs:** En cumplimiento del RGPD y de las normas ISO 27001 e ISO 27701, NORMON realiza de manera sistemática evaluaciones de riesgos relacionadas tanto con la Seguridad de la Información como con las Actividades de Tratamiento de Datos Personales (RATs), así como Evaluaciones de Impacto en la Protección de Datos (EIPDs) cuando el tipo de tratamiento lo requiere o se identifican riesgos elevados para los derechos y libertades de las personas interesadas. Estas actividades permiten identificar y valorar los riesgos inherentes a cada activo de información y proceso de datos personales, estableciendo y aplicando medidas de mitigación acordes con los requisitos legales y los estándares internacionales de seguridad y privacidad. El procedimiento incluye la documentación detallada de los resultados, revisiones y actualizaciones periódicas ante cambios significativos en los tratamientos, el entorno regulatorio o el contexto organizativo. Asimismo, la integración de RATs y EIPDs en los procesos de gestión y la implementación de controles proporcionales al nivel de riesgo consolidan el compromiso de NORMON con la protección efectiva de la información, el cumplimiento normativo y la adopción de mejores prácticas internacionales en seguridad y privacidad.

6. **Compromiso con la Seguridad Integral**: NORMON considera la Seguridad Integral como un pilar fundamental para el logro de sus objetivos, asegurando la protección de los sistemas de información a través de la implantación, desarrollo y validación de planes de continuidad operativa que forman parte del Sistema de Continuidad de Negocio. Este enfoque permite garantizar la disponibilidad de la información y de los servicios críticos para los clientes en todo momento. Este compromiso se sustenta en una cultura organizacional orientada a la seguridad y privacidad de la información, promovida mediante acciones de formación y sensibilización dirigidas a todo el personal. La Seguridad Integral se gestiona de forma transversal en las siguientes áreas:
   - Seguridad Física: Protección de instalaciones, dependencias, sistemas hardware, soportes y cualquier activo físico relacionado con el tratamiento de información, así como controles de acceso físico.
   - Seguridad Lógica: Comprende la defensa de aplicaciones, redes, comunicaciones electrónicas, sistemas informáticos y los accesos lógicos correspondientes.

- Seguridad Político-Corporativa: Abarca los aspectos de seguridad inherentes a la organización, incluyendo normativas internas, regulaciones y cumplimiento de la legislación vigente.

La información gestionada por NORMON se clasifica y etiqueta en las siguientes categorías: ***pública, confidencial general, confidencial interno, confidencial acceso restringido y confidencial acceso restringido interno***. Esta clasificación facilita la gestión segura tanto de las comunicaciones internas como externas, así como de la información almacenada y en tránsito, garantizando que cada tipo de dato reciba un nivel de protección acorde a su sensibilidad. Entre las medidas técnicas y organizativas implementadas se incluyen: la seudonimización y el cifrado de datos, el control de accesos basado en roles y políticas de autenticación multifactor (MFA), la gestión segura de soportes y dispositivos, el registro y la monitorización de actividades, la formación continua del personal en materia de protección de datos y la adecuada gestión de incidentes de seguridad. Además, se fomenta la integración del principio de privacidad desde el diseño y por defecto, asegurando que cualquier nuevo tratamiento o sistema incorpore salvaguardas apropiadas desde su fase inicial.

7. Asignación de Responsabilidades y Roles: Las responsabilidades en materia de seguridad de la información y privacidad están claramente definidas y asignadas a todos los niveles de la organización, conforme a la estructura organizativa y los procedimientos internos:
   - Consejo de Administración: Aprueba la política y supervisa el grado de cumplimiento.
   - Dirección General: Lidera la implantación y provisión de recursos para el sistema de gestión.
   - Comité de Seguridad de la Información: Coordina, evalúa y revisa las iniciativas y controles de seguridad y privacidad.
   - Delegado de Protección de Datos (DPD): Supervisa el cumplimiento de la normativa de protección de datos, asesora y actúa como punto de contacto con interesados y autoridades.
   - Responsable de Seguridad de la Información (CISO): Dirige la estrategia de seguridad, gestiona los riesgos y supervisa la implementación de controles de protección.
   - Responsable del Dato: Garantiza la correcta gestión y protección de los datos conforme a la normativa vigente.
   - Responsable de Transformación Digital: Lidera los proyectos de digitalización de la organización, impulsa la adopción de nuevas tecnologías y coordina la integración de soluciones innovadoras para optimizar procesos, garantizar la seguridad y promover la eficiencia en línea con los objetivos estratégicos.
   - Responsable de Seguridad del Servicio IT: Se encarga de la protección de los sistemas y servicios tecnológicos, asegurando su resiliencia y continuidad.
   - Responsable de Seguridad del Servicio OT: Supervisa la seguridad de los sistemas operacionales y tecnológicos industriales.
   - Responsable del Sistema de Gestión del Servicio IT: Administra y optimiza los procesos relacionados con la gestión de servicios tecnológicos.
   - Responsable de Gestión del Sistema de Seguridad de la Información: Coordina el mantenimiento y la mejora continua del sistema de gestión de seguridad.
   - Responsables de Departamentos: Velan por la aplicación de las políticas y procedimientos en sus ámbitos de competencia.
   - Personas trabajadoras: Deben conocer y cumplir las obligaciones y buenas prácticas establecidas en la política y procedimientos. La formación y sensibilización en materia de seguridad y privacidad es obligatoria y continua para todo el personal, con el fin de garantizar la competencia y el compromiso necesarios.

8. Procedimiento para el Tratamiento de Exenciones y Excepciones: De conformidad con el Control 5.1 de la Norma UNE-EN-ISO/IEC 27002:2023, cualquier exención o excepción a esta Política o a los

procedimientos asociados deberá ser solicitada formalmente por el responsable del área afectada, motivando la necesidad y el alcance de la exención. El procedimiento será el siguiente:

1) Presentación de la solicitud de exención o excepción, debidamente justificada, ante el Comité de Seguridad de la Información.
2) Evaluación de la solicitud por el Comité, considerando los riesgos, impactos y salvaguardas alternativas.
3) Decisión motivada del Comité, que podrá aprobar, rechazar o solicitar modificaciones a la solicitud.
4) Registro documental de la exención o excepción autorizada, incluyendo condiciones, plazo y responsables de seguimiento.
5) Comunicación de la decisión a las partes interesadas y revisión periódica de las exenciones concedidas.

9. Protección de las Partes Interesadas: La protección de la información y los datos personales de clientes, proveedores, personas trabajadoras y demás partes interesadas es prioritaria para NORMON. Para ello, se implementan medidas técnicas, operativas y organizativas adecuadas, así como cláusulas contractuales específicas en las relaciones con terceros. En cumplimiento del RGPD, mantenemos y actualizamos los RATs obligatorios, asegurando la trazabilidad y transparencia en el uso de los datos personales. Además, se desarrolla y mantiene actualizado el Manual de Seguridad de la Información y de Gestión de la Privacidad, que recoge los procedimientos, instrucciones técnicas y controles necesarios para garantizar la seguridad y la privacidad, conforme a la estructura y requisitos del SGSI.

10. Mejora Continua: NORMON asume la mejora continua del SGSI como pilar esencial, mediante la definición de objetivos medibles, la monitorización de indicadores clave, auditorías internas y externas, revisiones de la dirección y la adopción de mejores prácticas sectoriales. Se evalúa de forma regular la eficacia de las medidas implantadas y se establecen acciones de mejora para elevar el nivel de madurez y resiliencia del sistema.

11. Formación y Concienciación: En el marco de la política de seguridad de la información y gestión de la privacidad de NORMON, se implementa un programa obligatorio y permanente de formación y sensibilización dirigido a todo el personal. Este programa persigue asegurar que todas las personas trabajadoras dispongan de las competencias actualizadas y necesarias para proteger los datos personales, cumplir con la normativa vigente, gestionar de forma segura los servicios de IT y utilizar tecnologías, incluida la inteligencia artificial, de manera ética y segura. La formación se revisa y actualiza periódicamente para responder a las modificaciones normativas, avances tecnológicos y cambios organizativos, fomentando así una cultura corporativa de seguridad y privacidad plenamente alineada con los principios y requisitos del SGSI de la organización.

12. Aplicabilidad, Disponibilidad y Difusión: Esta política es de obligado cumplimiento para todo el personal y áreas de NORMON, estando disponible para su consulta en todos los niveles organizativos y por las partes interesadas que lo soliciten. Su difusión se garantiza a través de los canales corporativos y el repositorio documental interno, facilitando el acceso tanto al equipo interno como a las partes externas interesadas. La política será revisada al menos una vez al año, o siempre que se produzcan cambios significativos en el marco normativo, tecnológico u organizativo, y se actualizará en función de los resultados de dichas revisiones y de la evolución de los riesgos detectados.

13. Reflexión sobre Integración o Separación de Políticas: La integración de las políticas de seguridad de la información y de gestión de la privacidad en un marco común presenta ventajas significativas, como la optimización de recursos, la coherencia en la aplicación de controles y la alineación estratégica de los objetivos de protección de la organización. No obstante, también es importante considerar las diferencias inherentes entre ambas disciplinas: mientras la seguridad de la información abarca la

protección de todos los activos informacionales, la gestión de la privacidad se centra específicamente en los datos personales y en el cumplimiento de los requerimientos legales asociados.

14. **Compromiso de la Dirección:** El Consejo de Administración, la Dirección General y el Comité de Seguridad de la Información de NORMON reafirman su compromiso en liderar la implantación de esta política, impulsando la participación y responsabilidad de toda la organización para alcanzar los objetivos establecidos.

Aprobado por Dirección General

Noviembre 2025