PROTOCOLO DE USO DE INTELIGENCIA ARTIFICIAL, PROTECCIÓN DE DATOS Y GESTIÓN DE LA INFORMACIÓN PARA EMPLEADOS GRUPO EMPRESARIAL GRUPO SATOCAN [“GRUPO SATOCAN”]

1.- INTRODUCCIÓN Y OBJETO

El presente protocolo tiene como objetivo establecer las directrices y normas de obligado cumplimiento para todos los empleados del Grupo, [en adelante “**GRUPO SATOCAN**”] en relación con el **uso de las herramientas de Inteligencia Artificial (IA), la protección de datos personales, la gestión de la información y la prevención de riesgos legales**.

La Empresa ha realizado una **importante inversión en tecnologías de IA para optimizar nuestros procesos, mejorar la eficiencia y potenciar la innovación en todos nuestros Departamentos y unidades de negocio** (Hoteles, Plantas, etc.…). Sin embargo, el uso indebido de estas herramientas, así como una gestión negligente de la información, puede acarrear graves riesgos legales y reputacionales para la Empresa y para nuestros empleados.

Este protocolo busca **garantizar un uso responsable, ético y legal de la IA y de la información, protegiendo los derechos de terceros, la privacidad y la confidencialidad de nuestros datos, y asegurando el cumplimiento de la normativa vigente**, incluyendo el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y cualquier otra legislación aplicable en materia de propiedad intelectual, seguridad de la información y buen gobierno corporativo.

2.- ÁMBITO DE APLICACIÓN

Este protocolo es de obligado cumplimiento para la totalidad de la plantilla del Grupo Empresarial **[“GRUPO SATOCAN”],** incluyendo directivos, mandos intermedios, empleados, personal temporal, becarios y colaboradores externos que, en el desarrollo de sus funciones, tengan acceso o hagan uso de las herramientas de IA implementadas por la Empresa o gestionen cualquier tipo de información corporativa.

3.-PRINCIPIOS GENERALES

Todos los empleados deberán observar los siguientes principios en el desarrollo de sus funciones y en el uso de las herramientas de IA:

- Legalidad: Cumplimiento estricto de toda la normativa aplicable.
- Ética y Responsabilidad: Uso de la IA de forma ética, justa y sin discriminación. Asumir la responsabilidad por las acciones y decisiones tomadas con el apoyo de la IA.
- Confidencialidad: Protección de la información confidencial de la Empresa, clientes y terceros.
- Privacidad: Respeto y protección de la privacidad de los datos personales.
- Precisión y Verificación: No asumir que la información generada por la IA es siempre precisa. Verificación y validación de la información antes de su uso o difusión.
- Seguridad: Adopción de medidas de seguridad para proteger los sistemas de IA y la información que procesan.

4.- USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL (IA)

4.1. Herramientas de IA corporativas:

* Los empleados deben utilizar exclusivamente las herramientas de IA proporcionadas y autorizadas por la Empresa.

4.2. Datos e información a introducir en sistemas de IA:

* Prohibición de datos personales sensibles: Nunca se deben introducir en ninguna herramienta de IA (tanto interna como externa) datos personales sensibles, como datos de salud, origen étnico o racial, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos, u orientación sexual.

* Información confidencial de la Empresa: No se debe introducir información estratégica, financiera, técnica (planos, diseños de proyectos, etc.), comercial o de cualquier otra índole que sea considerada confidencial por la Empresa, en herramientas de IA que no hayan sido aprobadas para el manejo de dicha información, y bajo condiciones de seguridad y confidencialidad garantizadas.

* Propiedad Intelectual: No se deben introducir en herramientas de IA de acceso público o de terceros, contenidos sobre los que la Empresa posea derechos de propiedad intelectual (ej. diseños arquitectónicos, planes de marketing, software propio, etc.)

4.3. Uso de imágenes y contenido audiovisual generado por IA:

Para la generación o edición de imágenes, vídeos o cualquier otro contenido audiovisual, se deberán utilizar exclusivamente las herramientas de Inteligencia Artificial aprobadas y proporcionadas por la empresa. Estas herramientas han sido seleccionadas por ofrecer garantías adecuadas en materia de derechos de autor y privacidad. El empleado deberá, además, seguir las buenas prácticas de uso establecidas por la compañía.

* En caso de que las imágenes o vídeos incluyan personas identificables, se deberá contar con la autorización previa de dichas personas, o asegurarse de que su uso se enmarca dentro de una excepción legal (ej. uso en lugares públicos con fines informativos y no comerciales, cuando la persona sea un elemento secundario o incidental).

* Se prohíbe el uso de IA para generar o manipular imágenes o vídeos que puedan resultar difamatorios, ofensivos, discriminatorios o que puedan dañar la reputación de la Empresa o de terceros.

4.4. Implicaciones en la facturación y procesos financieros:

* Cualquier uso de IA que impacte en la generación, procesamiento o validación de facturas o cualquier documento financiero debe ser supervisado y validado por el departamento correspondiente (Administración/Finanzas) para asegurar la integridad, exactitud y legalidad de las operaciones.

5.- PROTECCIÓN DE DATOS PERSONALES

5.1. Recopilación y tratamiento de datos:

* Todos los empleados deben cumplir con las políticas de protección de datos de la Empresa, que se basan en el RGPD y la LOPDGDD.

* Solo se podrán recopilar y tratar datos personales cuando exista una base legal legítima para ello (consentimiento del interesado, ejecución de un contrato, cumplimiento de una obligación legal, interés vital o interés legítimo de la Empresa).

* Los datos personales deben ser tratados de forma lícita, leal y transparente.

5.2. Finalidad y minimización:

* Los datos personales deben ser recopilados con fines específicos, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

* Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (principio de minimización de datos).

5.3. Exactitud y conservación:

* Los datos personales deben ser exactos y, si fuera necesario, actualizados.

* Los datos no se conservarán durante más tiempo del necesario para los fines para los que fueron recopilados, o para cumplir con obligaciones legales.

5.4. Confidencialidad e integridad:

* Se deben implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales y protegerlos contra el tratamiento no autorizado o ilícito, la pérdida, destrucción o daño accidental.

* Todos los empleados tienen la obligación de mantener la confidencialidad de los datos personales a los que tengan acceso.

5.5. Ejercicio de derechos ARCO-POL:

* Cualquier solicitud de ejercicio de derechos (Acceso, Rectificación, Cancelación/Supresión, Oposición, Portabilidad y Limitación del tratamiento) recibida por un empleado debe ser remitida de inmediato al Departamento Legal o directamente al Delegado de Protección de Datos (DPD) de la Empresa, cuya dirección de correo electrónico es la siguiente: aperez@prodat.es.

6.- SEGURIDAD DE LA INFORMACIÓN

6.1. Contraseñas y acceso:

* Los empleados son responsables de mantener la confidencialidad de sus credenciales de acceso (nombres de usuario y contraseñas) a todos los sistemas y herramientas de la Empresa.

* Las contraseñas deben ser robustas y no ser compartidas bajo ninguna circunstancia.

6.2. Uso de dispositivos:

* El uso de dispositivos personales para acceder a la información corporativa o a las herramientas de IA solo está permitido si cumple con las políticas de seguridad de la Empresa.

* Se prohíbe el uso de dispositivos no autorizados para el almacenamiento o tratamiento de información confidencial.

6.3. Información en tránsito:

* Se deben utilizar los canales seguros y autorizados por la Empresa para la transferencia de información confidencial o datos personales.

* Evitar el envío de información sensible por correo electrónico sin cifrado o a través de redes Wi-Fi públicas no seguras.

7.- FORMACIÓN Y CONCIENCIACIÓN

La Empresa se compromete a proporcionar la formación necesaria a aquellos empleados que lo precisen para el correcto desarrollo de su trabajo, sobre el uso adecuado de las herramientas de IA, las políticas de protección de datos y las mejores prácticas en seguridad de la información. La asistencia a estas formaciones es obligatoria para todos los empleados.

8.- CLASIFICACIÓN DE SISTEMAS Y APLICACIONES

Con el objetivo de garantizar un uso seguro, ético y conforme a la normativa vigente, la empresa ha procedido a analizar y clasificar aquellos sistemas y aplicaciones de Inteligencia Artificial (IA) que vayan a ser utilizados, antes de su implementación o uso generalizado. Esta clasificación se basa en los niveles de riesgo definidos por el Reglamento de Inteligencia Artificial de la Unión Europea, y se irán actualizando a medida que se implante o utilicen otros sistemas y/o aplicaciones.

El Departamento de IT, en colaboración con el Departamento Legal y los responsables de cada área, será el encargado de evaluar cada herramienta de IA. Se mantendrá un **registro interno y actualizado** con la clasificación de todas las aplicaciones permitidas, que será de consulta obligatoria para todos los empleados.

Se acompaña como **Anexo I,** la clasificación actual, que se irá actualizando a medida que se vayan implementando nuevas aplicaciones/herramientas de IA.

9.- COMITÉ DE CUMPLIMIENTO

Con el fin de garantizar el cumplimiento del presente Protocolo, de la normativa vigente y futura en materia de Inteligencia Artificial, y de velar por la resolución de cuestiones éticas vinculadas al uso de la IA en el seno del Grupo, se nombrará un Comité de Cumplimiento en materia de Inteligencia Artificial (en adelante, el **"Comité"**).

El Comité será nombrado por el órgano de administración del Grupo y estará compuesto por un mínimo de tres (3) miembros, garantizando un perfil multidisciplinar que abarque aspectos legales, técnicos y éticos.

El Comité actuará de forma independiente, reportando directamente al órgano de administración, y su labor se centrará en la supervisión y promoción de un uso responsable, ético y legal de la Inteligencia Artificial en todas las operaciones del Grupo.

Las funciones específicas del Comité serán las siguientes:

i. **Supervisión y Monitorización:** Supervisar la implementación y el cumplimiento de las directrices establecidas en este Protocolo, así como de las obligaciones derivadas de la normativa aplicable en materia de Inteligencia Artificial, incluyendo el Reglamento Europeo de Inteligencia Artificial (RIA).

ii. **Asesoramiento y Consulta:** Actuar como órgano consultivo para todos los departamentos y empleados del Grupo en relación con las dudas y cuestiones que puedan surgir en el uso de herramientas de IA y la gestión de la información.

iii. **Gestión de Riesgos:** Colaborar con el Departamento Jurídico en la identificación, evaluación y mitigación de los riesgos legales, éticos y reputacionales asociados al uso de la IA, incluyendo la aprobación de modelos de evaluación de riesgo para sistemas de IA, especialmente los de alto riesgo.

iv. **Formación y Concienciación:** Proponer y supervisar los programas de formación y concienciación para los empleados sobre el uso adecuado de la IA, la protección de datos y la seguridad de la información.

v. **Actualización Normativa:** Realizar un seguimiento continuo de la evolución legislativa y tecnológica en el ámbito de la Inteligencia Artificial, proponiendo las actualizaciones y modificaciones necesarias al presente Protocolo.

vi. **Gestión de Denuncias:** Gestionar y tramitar las denuncias recibidas a través del canal de denuncias éticas interno del Grupo, relativas a posibles usos indebidos de la IA, vulneraciones de datos o riesgos de seguridad, velando por el cumplimiento de las garantías y la confidencialidad de los denunciantes. El Comité será el encargado de investigar las incidencias y proponer las acciones correctivas o disciplinarias que correspondan.

vii. **Aprobación de Herramientas de IA:** Colaborar con los Departamentos de IT y Jurídico en la validación y aprobación de las herramientas de IA corporativas y de terceros antes de su implementación y uso, asegurando su conformidad con los principios del Protocolo y la normativa.

viii. **Evaluación de Impacto en Derechos Fundamentales:** Para las sociedades del Grupo que presten servicios públicos o que desarrollen cualquier contrato con la Administración, realizar la evaluación del impacto que la utilización de sistemas de IA de alto riesgo puede tener en los derechos fundamentales antes de su despliegue, y, en su caso, notificar los resultados a la autoridad correspondiente.

Se acompaña como **Anexo II**, Acta de nombramiento formal de los miembros del Comité de Cumplimiento, el detalle de su composición y reglas de funcionamiento.

10.- INCUMPLIMIENTO Y CONSECUENCIAS

El incumplimiento de lo establecido en este protocolo será considerado una falta grave y podrá dar lugar a la imposición de sanciones disciplinarias, de conformidad con la legislación laboral vigente y el convenio colectivo aplicable, pudiendo llegar, en los casos más graves, a la extinción de la relación laboral.

Adicionalmente, el empleado podrá ser considerado responsable de las consecuencias legales derivadas de su incumplimiento, incluyendo responsabilidades civiles, penales o administrativas.

11.- REVISIÓN DEL PROTOCOLO

Este protocolo será revisado periódicamente por el Departamento Legal y de IT de la Empresa para asegurar su adecuación a las novedades legislativas, tecnológicas y las necesidades operativas de la Empresa.

12.- CANALES DE CONSULTA Y DENUNCIA

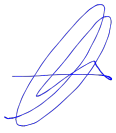
Ante cualquier duda sobre la aplicación de este protocolo, los empleados deben dirigirse al Departamento Legal o al Departamento de IT.

Cualquier incidencia, sospecha de uso indebido de la IA, vulneración de datos o riesgo de seguridad debe ser comunicada de inmediato a través del canal de denuncia interno establecido por la Empresa o directamente al Departamento Legal/DPD.

En Las Palmas de Gran Canaria, a 1 de octubre de 2025

D. José Julio Artiles Moragas

D. Pablo Mariño Vila



D. Miguel Quintanilla Eriksson

D. Aday Hernández Vieira

Dña. Judith Vega Martínez

Fdo: José Julio Artiles Moragas