**POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (SSI)**

**Brambati SpA** considera la Seguridad de los Sistemas de Información (SSI) un elemento estratégico para la protección de sus datos, procesos y relaciones con clientes, proveedores y partes interesadas. Esta Política es consistente con los principios de las Directivas europeas NIS2 y REC, está inspirada en las mejores prácticas de la norma ISO/IEC 27001 e integra los requisitos del Sistema de Gestión Integrado de la empresa.

**Principios fundamentales**

Los principios fundamentales que guían la gestión de la seguridad de la información en **Brambati SpA** se basan en:

* Disponibilidad → garantizar que los sistemas y la información sean accesibles y utilizables cuando lo requieran los procesos de negocio y los usuarios autorizados;
* Integridad → garantizar la exactitud, integridad y fiabilidad de los datos y la información a lo largo de su ciclo de vida;
* Confidencialidad → proteger la información del acceso no autorizado, garantizando que sólo las partes autorizadas puedan acceder a ella y procesarla.

**Gestión de los riesgos**

**Brambati SpA** adopta un enfoque sistemático de Análisis de Riesgos y Oportunidades para identificar, evaluar y mitigar las amenazas a la seguridad de la información, considerando también el impacto del cambio climático y los eventos extremos en la continuidad de los sistemas TIC. En particular se analizan los siguientes:

* Ataques cibernéticos (malware, ransomware, phishing, accesos no autorizados);
* Fallas técnicas, apagones e indisponibilidad de sistemas críticos;
* Eventos naturales y climáticos que pueden comprometer la infraestructura y los centros de datos;
* Riesgos derivados de proveedores externos, socios y la cadena de suministro digital;
* Errores humanos y falta de concienciación del personal.

Las oportunidades identificadas incluyen:

* Adopción de tecnologías innovadoras y seguras (nube resiliente, IA, blockchain);
* Desarrollo de una cultura de ciberseguridad corporativa a través de capacitación continua;
* Mayor confianza de los clientes y las partes interesadas a través de sistemas seguros y confiables;
* Resiliencia organizacional y capacidad de respuesta rápida ante incidentes y crisis.

**Compromisos de gestión**

La gestión de **Brambati SpA** se compromete a:

* Garantizar el cumplimiento de las leyes, regulaciones y directivas aplicables (NIS2, REC, GDPR, Código de privacidad);
* Definir objetivos y programas de mejora de la seguridad de la información;
* Garantizar recursos, roles y responsabilidades para la gestión de la seguridad;
* Revisar periódicamente esta Política y el sistema de seguridad de la información para verificar su eficacia y adecuación;
* Integrar los principios de seguridad por diseño y por defecto en el desarrollo y gestión de procesos y sistemas de información;
* Promover la concientización y capacitación de todo el personal sobre seguridad de la información.

**Objetivos operativos**

Los objetivos operativos que **Brambati SpA** se fija en materia de SSI incluyen:

* Proteger los datos personales, industriales y de propiedad contra el acceso y procesamiento no autorizados;
* Garantizar la continuidad del negocio y las capacidades de recuperación rápida a través de planes de continuidad del negocio y recuperación ante desastres;
* Monitorear continuamente los sistemas para detectar y responder con prontitud a incidentes de seguridad;
* Gestionar correctamente el acceso, las identidades digitales y los privilegios de los usuarios;
* Realizar copias de seguridad seguras de forma periódica y pruebas de restauración;
* Evaluar y supervisar a proveedores críticos y servicios subcontratados para garantizar la alineación con los estándares de seguridad corporativa.

**Monitoreo y mejora**

**Brambati SpA** garantiza la monitorización constante y la mejora continua de la seguridad de los sistemas de información a través de:

* Definición y seguimiento de KPI (incidentes gestionados, tiempos promedio de recuperación, % capacitación completada, disponibilidad de sistemas críticos);
* Auditorías internas y externas para verificar el cumplimiento de las políticas y estándares de seguridad;
* Análisis periódico de amenazas y actualización de contramedidas técnicas y organizativas;
* Participación activa de la dirección y de los responsables operativos en los procesos de toma de decisiones relacionados con el SSI.

**Integración en el uso de la Inteligencia Artificial (IA)**

**Brambati SpA**, aunque no desarrolla sistemas de Inteligencia Artificial, los utiliza en algunos procesos de gestión, producción y soporte. Por este motivo, la empresa reconoce la importancia de garantizar que estas herramientas se utilicen de forma segura, responsable y de conformidad con la legislación europea, en particular el Reglamento (UE) AI Act y el RGPD.

En relación con el uso de herramientas de IA, **Brambati SpA** se compromete a:

* Aplicar los principios fundamentales de disponibilidad, integridad y confidencialidad a los datos y algoritmos utilizados por los sistemas de IA;
* Evaluar y mitigar los riesgos relacionados con el sesgo, la discriminación algorítmica y la opacidad de las decisiones automatizadas;
* Verificar el cumplimiento de los proveedores de soluciones de IA con las regulaciones europeas y los estándares éticos de la industria;
* Garantizar la transparencia y la rendición de cuentas en el uso de herramientas de IA, garantizando que las decisiones críticas nunca se confíen exclusivamente a sistemas automatizados;
* Integrar la IA en los procesos de capacitación, auditoría y monitoreo de seguridad de los sistemas de información.

Esta Política de Seguridad de los Sistemas de Información se difunde a todo el personal, se pone a disposición de las partes interesadas y se publica en el sitio web de la empresa. Representa el compromiso formal de **Brambati SpA** proteger sus activos de información, garantizando la disponibilidad, integridad y confidencialidad, y perseguir la mejora continua en la seguridad de informática.

 Fecha Dirección **Brambati SpA**

Codevilla, 01/09/2025 ………………………………….