ÍNDICE

1. INTRODUCCIÓN 2
2. ALCANCE 4
3. MISIÓN 4
4. MARCO NORMATIVO 4
5. ROLES: FUNCIONES Y RESPONSABILIDADES 5
6. DATOS DE CARÁCTER PERSONAL 6
7.OBLIGACIONES DEL PERSONAL 6
8.TERCERAS PARTES 6
9. APROBACIÓN 7
10. HISTORIAL DE REVISIONES 7

		Firma:	Fecha:
CREADO:	Responsable De SGSI	Sergi Hidalgo	21/10/2024
APROBADO:	Dirección/Resp. Información Y Servicio	Toni Hidalgo	25/04/2025

1. INTRODUCCIÓN

HIGIA BENCHMARKING S.L., en adelante BENCHMARKING es una empresa especializada en software y servicios de información en el ámbito de la gestión clínica y sanitaria para centros de salud, cuyos principales valores son la red BENCHMARKING SANITARIO 3.0 (BS3), en la cual participan más de 190 hospitales, tanto públicos como privados, de toda España, y los BEST SPANISH HOSPITALS AWARDS (PREMIOS BSH).

Desde su constitución, el objetivo de BENCHMARKING es prestar un servicio a sus clientes cumpliendo los requisitos establecidos, de forma que obtengan la máxima satisfacción con nuestros servicios y se garantice la máxima privacidad y seguridad de la información de nuestra empresa.

Dicho objetivo de satisfacción de nuestros clientes y confidencialidad de la información es la piedra angular de nuestra política, entendiendo la satisfacción como el cumplimiento de los compromisos contraídos de la forma más eficiente posible, a la vez que se procura cumplir con las expectativas no contractuales derivadas de las necesidades descubiertas en la ejecución del servicio y relacionadas con el mismo, que el propio cliente nos comunica.

Mediante la aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en los requisitos de las normas ISO/IEC 27001:2022, se persigue una mejora continua en la calidad de los servicios y continuidad de los mismos de las actividades que desarrolla nuestra organización, así como un compromiso continuo de mejora técnica de nuestros sistemas, activos y procesos y el de nuestros proveedores, para procurar una continua adaptación a las necesidades tecnológicas de nuestros clientes.

Para ello, BENCHMARKING, considera la base de esta Política como pilares básicos de la organización para alcanzar la mejora continua de la eficacia de dicho sistema de Gestión, las siguientes directrices, que servirán de base al establecimiento de nuestros objetivos anuales:

- Asegurar la satisfacción de sus clientes basándose en un trato siempre correcto y en un esfuerzo continuo en la prestación del servicio en base a sus requisitos y a nuestros compromisos de actualizaciones y mejoras.
- Cumplir con los requisitos de los clientes y de sus grupos de interés, así como con los requisitos legales y reglamentarios que afecten a la realización y prestación de los servicios prestados.
- Cumplir con los requisitos legales que le son de aplicación, así como con aquellos requisitos que la organización suscriba evaluando continuamente dicho cumplimiento, en todas sus áreas de actividad.
- Evaluar de forma concienzuda los riesgos de la organización, analizando los posibles riesgos de todos y cada uno de los procesos de la organización y de los activos de información, previendo y evitando de esta manera desviaciones, tomando las oportunas decisiones para minimizar posibles no conformidades.
- Establecer procesos operacionales que salvaguarden a las personas, la propiedad, la información, los datos y las aplicaciones o sistemas de uso para las instancias establecidas por la organización.
- Velar por una continua y permanente actualización de nuestros recursos, tanto tecnológicos como, sobre todo, de nuestro personal, fomentando políticas de información y formación continua profesional que les permitan avanzar en sus conocimientos al ritmo que lo hace nuestro sector, fomentando la conciencia de la seguridad de la información, a fin de incrementar la competencia de los empleados.
- Establecer y revisar regularmente los Objetivos, acordes con los compromisos que se asumen en esta declaración, fortaleciendo el compromiso y participación de todo el personal en el desarrollo y consecución de los Objetivos.
- Garantizar la mejora continua, manteniendo el Sistema de forma eficaz y efectiva para constatar el compromiso con los clientes, buscando para ello una mejor organización interna del trabajo y en la forma en que tratamos la información de nuestros clientes.
- Lograr que la seguridad de la información y el respeto a los datos personales sean una constante:
    - Preservando la confidencialidad de la información y evitando su divulgación y el acceso por personas no autorizadas.

- Manteniendo la integridad de la información procurando su exactitud y evitando su deterioro.
- Asegurando la disponibilidad de la información en todos los soportes y siempre que sea necesaria.

- La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos la valoración de la disponibilidad, confidencialidad e integridad de su información y aún más la de sus clientes.

2. ALCANCE

La organización establece para la norma ISO/IEC 27001:2022 esta política que se aplica a *los sistemas de información que dan soporte a: Los sistemas de gestión de seguridad de la información que dan soporte a la solución integral de análisis y aprovechamiento de la información del CMBD para mejorar el rendimiento, la eficiencia y la calidad en la prestación de servicios de salud.*

3. MISIÓN

La misión de BENCHMARKING es prestar servicios TIC, relacionados con soluciones tecnológicas multisectoriales, con un equipo humano comprometido con el cliente, ilusionado con su desarrollo profesional, apoyado en una tecnología avanzada, moderna y segura.

4. MARCO NORMATIVO

BENCHMARKING se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general (Código Civil, Código de comercio, etc.) o específico, como por ejemplo la siguiente:

- ISO/IEC 27001:2022 y 27002:2022 como normas marco del SGSI.
- Reglamento General de Protección de Datos (RGPD – UE 2016/679).
- Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).
- Ley 9/2017, de Contratos del Sector Público (cuando aplique).

- Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- Ley 34/2002 de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
- Ley 39/2015 de 1 de Octubre, Procedimiento Administrativo Común de las Administraciones Públicas

5. ROLES: FUNCIONES Y RESPONSABILIDADES

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 a las que obliga la norma ISO 27001:2022 para verificar el cumplimiento.
- Gestionar o promover la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existentes son las adecuadas para las necesidades de la entidad, con la colaboración de los distintos responsables de sistemas IT/OT.
- Revisar, completar y aprobar, junto al Responsable de Información/Dirección, toda la documentación relacionada con la seguridad del sistema, con el auxilio del resto del Comité de Seguridad.
- La especificación de requisitos de seguridad corresponde a los responsables de la información y de los servicios, junto con el responsable del registro de actividades de datos de carácter personal. La operación corresponde a los responsables de los sistemas, mientras que la supervisión corresponde al responsable de la seguridad y al técnico de seguridad.

La descripción concreta de todas las responsabilidades puede consultarse en el documento Anexo Funciones y Responsabilidades.

Por su parte, el personal de la empresa tiene identificadas y comunicadas sus responsabilidades con relación a la seguridad de la información entre las que se destacan:

- Comunicar las incidencias de seguridad mediante los canales establecidos.
- Aplicar los mecanismos establecidos para el intercambio de información entre el personal, clientes y proveedores.

Cualquier asignación de tareas y responsabilidades de seguridad de la información será aprobada por el Comité de Seguridad.

6. DATOS DE CARÁCTER PERSONAL

BENCHMARKING, trata los datos de carácter personal, por lo que mantiene “un registro de actividades de tratamiento”, al que tendrán acceso sólo las personas autorizadas, en el que se recogen los datos afectados y los responsables del tratamiento. Todos los sistemas de información de BENCHMARKING 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 registro.

7.OBLIGACIONES DEL PERSONAL

Todos los trabajadores de BENCHMARKING tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de BENCHMARKING., en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance 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, por el contrario, se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

8.TERCERAS PARTES

Las terceras partes relacionadas con BENCHMARKING, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando BENCHMARKING utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte, quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

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.

9. APROBACIÓN

Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

10. HISTORIAL DE REVISIONES

Esta Política será revisada para su continua adecuación anualmente por la Dirección, así como los objetivos y metas de la empresa, y comunicada a todo el personal de la organización encontrándose a disposición del público bajo solicitud de cualquier parte interesada.

Revisión	Fecha	Razón Modificación
1.0	23/10/2024	Creación del Documento
1.1	25/04/2025	Adaptación a una nueva estructura

La Dirección se asegura que la Política de Seguridad de la Información es entendida, implantada y mantenida al día en todos los niveles de la Organización.

En Barcelona, a 25 de abril de 2025

Fdo.: Toni Hidalgo
CEO