Política de Seguridad de la Información de Higia Benchmarking SL

Benchmarking Sanitario 3.0
Best Spanish Hospitals Awards

BENCHMARKING Sanitario 3.0

Contenido

1. Introducción

HIGIA BENCHMARKING SL 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 180 hospitales, tanto públicos como privados, de toda España, y los BEST SPANISH HOSPITALS AWARDS (PREMIOS BSH).

HIGIA BENCHMARKING SL, reconoce la importancia de proteger la información sensible y confidencial de sus clientes y de garantizar la disponibilidad, integridad y confidencialidad de los datos.

Con la implementación de este Política de Seguridad de la Información, HIGIA BENCHMARKING SL pretende establecer los controles y las medidas necesarias que deberán ser aplicadas para proteger los activos de información de la empresa.

2. Alcance

Esta política se aplicará a todos los empleados, contratistas, colaboradores y terceros que tengan acceso a los activos de información de HIGIA BENCHMARKING SL. Además, cubrirá todos los sistemas, infraestructuras, redes, dispositivos, aplicaciones y procesos utilizados en la empresa.

3. Responsabilidades

3.1 Alta Dirección

La Alta Dirección de HIGIA BENCHMARKING SL será responsable de establecer una cultura de seguridad de la información en toda la organización. Deberá asignar los recursos necesarios para implementar y mantener controles de seguridad efectivos, garantizar el cumplimiento del ENS y proporcionar el liderazgo y apoyo adecuados para la seguridad de la información.

3.2 Responsable de Seguridad de la Información (RSI)

El RSI tendrá la responsabilidad de desarrollar, implementar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) en HIGIA BENCHMARKING SL. Esto incluye establecer y revisar políticas y procedimientos de seguridad, realizar evaluaciones de riesgos, coordinar actividades de seguridad, proporcionar capacitación y concienciación en seguridad de la información, y garantizar el cumplimiento de las regulaciones y normativas aplicables.

3.3 Empleados y Usuarios

Todos los empleados de HIGIA BENCHMARKING SL, así como sus usuarios, tendrán la responsabilidad de cumplir con esta Política de Seguridad de la Información. Deberán participar en programas de formación y concienciación en seguridad de la información, informar sobre cualquier incidente o violación de seguridad de inmediato, y seguir los controles y procedimientos establecidos para proteger los activos de información.

3.4 Uso Seguro de Dispositivos Móviles y BYOD

Se establecerán políticas y procedimientos específicos para el uso seguro de dispositivos móviles y la implementación del programa BYOD (Bring Your Own Device), si corresponde. Esto incluye el cifrado de datos en dispositivos móviles, la instalación de aplicaciones seguras, el uso de conexiones VPN para acceder a la red corporativa, y la protección de dispositivos en caso de pérdida o robo.

4. Gestión de Activos de Información

4.1 Inventario de Activos

Se dispondrá de un inventario exhaustivo de todos los activos de información de HIGIA BENCHMARKING SL, incluyendo servidores, sistemas, aplicaciones, bases de datos, dispositivos móviles y cualquier otro activo relacionado con la información. El inventario se actualizará regularmente y se mantendrá bajo la responsabilidad del RSI.

4.2 Clasificación de Activos

Los activos de información se clasificarán de acuerdo con su importancia, sensibilidad y valor para HIGIA BENCHMARKING SL y sus clientes. Se establecerán niveles de clasificación adecuados y se aplicarán controles de seguridad proporcionales a cada nivel de clasificación.

4.3 Propiedad de los Activos

Cada activo de información deberá tener un propietario designado, quien será responsable de su seguridad, protección y correcto uso. Los propietarios de los activos deberán garantizar que se implementen los controles de seguridad adecuados y que se realicen las acciones necesarias para mitigar los riesgos identificados.

4.4 Uso Aceptable de los Activos

Los activos de información de HIGIA BENCHMARKING SL solo deberán utilizarse para fines lícitos directamente relacionados con las actividades comerciales y de consultoría o producción de la empresa. Se deberán seguir las políticas y procedimientos establecidos para garantizar un uso adecuado y seguro de los activos, evitando el acceso no autorizado o los usos inapropiados.

4.5 Manejo de Soportes

Los soportes físicos y digitales que contengan información sensible deberán ser gestionados de manera segura. Se establecerán procedimientos para el manejo, transporte, almacenamiento y eliminación segura de los soportes, garantizando la confidencialidad e integridad de los datos.

4.6 Cumplimiento de la Ley de Protección de Datos

HIGIA BENCHMARKING SL se comprometerá a cumplir con todas las leyes y regulaciones aplicables en materia de protección de datos personales, incluyendo el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Se establecerán políticas y procedimientos para la recolección, uso, almacenamiento y eliminación segura de datos personales, así como para responder a solicitudes de derechos de los individuos y notificar violaciones de datos cuando ello corresponda.

5. Seguridad de los Recursos Personales

5.1 Contratación y Desvinculación

Se realizarán verificaciones de antecedentes y referencias para todos los nuevos empleados y contratistas antes de su contratación. Además, se implementarán procedimientos adecuados para desvincular a los empleados y contratistas, garantizando la devolución de los activos de información y la revocación de sus accesos.

5.2 Concienciación y Formación

Se llevarán a cabo programas de concienciación y formación en seguridad de la información para todos los empleados de HIGIA BENCHMARKING SL, que estarán también disponibles para sus usuarios. Estos programas incluirán temas como buenas prácticas de seguridad, manejo de contraseñas, uso seguro de dispositivos móviles, detección de phishing y otros ataques, y cumplimiento de políticas y regulaciones en materia de protección de datos.

5.3 Acuerdos de Confidencialidad

Se establecerán acuerdos de confidencialidad con todos los empleados y terceros que tengan acceso a información sensible de HIGIA BENCHMARKING SL o de sus clientes. Estos acuerdos establecerán claramente las responsabilidades y obligaciones de las partes en relación con la protección de la información confidencial.

5.4 Evaluación y gestión de Proveedores y Colaboradores

HIGIA BENCHMARKING SL establecerá criterios de evaluación de proveedores y colaboradores, incluyendo aspectos de seguridad de la información, antes de establecer relaciones comerciales con ellos. Se realizarán revisiones periódicas para asegurar que los proveedores y/o colaboradores cumplen con los requisitos de seguridad y protección de datos. Además, se establecerán acuerdos contractuales que garanticen la confidencialidad y seguridad de la información en caso de que sea lícito compartirla con ellos para el desarrollo de las actividades productivas de la empresa hacia sus clientes finales.

5.5 Uso Adecuado de Redes y Comunicaciones

HIGIA BENCHMARKING SL establecerá políticas y controles para garantizar el uso adecuado de las redes y comunicaciones de la empresa. Esto incluirá la implementación de medidas de seguridad en las redes, como firewalls y sistemas de detección de intrusiones, la protección de comunicaciones confidenciales mediante cifrado, el uso responsable de Internet y el filtrado de contenido no autorizado.

6. Control de Acceso

6.1 Política de Acceso

Se implementarán controles de acceso adecuados para garantizar que solo los usuarios autorizados tengan acceso a los activos de información de HIGIA BENCHMARKING SL. Esto incluye la asignación de permisos de acceso basados en roles, la autenticación de usuarios, el control de contraseñas, la supervisión de los accesos y la gestión de cuentas de usuario.

6.2 Gestión de Identidades y Accesos

Se establecerán procesos y procedimientos para gestionar de manera eficiente y segura las identidades y los accesos de los usuarios a los sistemas y aplicaciones de HIGIA BENCHMARKING SL. Esto incluirá la creación, modificación y revocación de cuentas de usuario, así como la revisión regular de los privilegios de acceso.

6.3 Control de Acceso Físico y Lógico

Se implementarán medidas de seguridad física y lógica para proteger los activos de información de HIGIA BENCHMARKING SL. Esto incluye el control de acceso a las instalaciones de la empresa, la protección de los dispositivos de almacenamiento y los servidores, y la supervisión de los registros de acceso para detectar actividades sospechosas.

6.4 Política de Contraseñas

Se establecerá una política de contraseñas sólida para garantizar contraseñas robustas y seguras. Esto incluirá requisitos mínimos de longitud, complejidad, cambio periódico de contraseñas, restricciones de reutilización y el uso de autenticación de doble factor cuando sea posible. Además, se promoverá la concienciación de los empleados, así como de los usuarios, sobre la importancia de mantener las contraseñas seguras y protegerlas de manera adecuada.

7. Seguridad en el Desarrollo y Mantenimiento de Sistemas

7.1 Ciclo de Vida de Desarrollo

Se implementará un enfoque seguro en el desarrollo de sistemas y aplicaciones, siguiendo buenas prácticas de seguridad desde la etapa de diseño hasta la implementación y mantenimiento. Se establecerán controles para garantizar la integridad de los sistemas, la autenticidad de los componentes y la protección contra vulnerabilidades conocidas.

7.2 Pruebas de Seguridad

Antes de la implementación de nuevos sistemas o actualizaciones importantes, se realizarán pruebas de seguridad exhaustivas para identificar posibles vulnerabilidades y debilidades. Se establecerán procesos para remediar las vulnerabilidades encontradas antes de la puesta en producción.

7.3 Gestión de Parches y Actualizaciones

Se establecerá un proceso formal para gestionar las actualizaciones de seguridad y los parches de los sistemas y aplicaciones utilizados por HIGIA BENCHMARKING SL. Esto incluirá la evaluación regular de las actualizaciones disponibles, la aplicación oportuna de los parches críticos y la comunicación efectiva con los usuarios afectados.

8. Seguridad en la Operación de los Sistemas

8.1 Monitorización y Registro de Eventos

Se implementará un sistema de monitorización y registro de eventos para detectar y responder rápidamente a incidentes de seguridad. Se establecerán procedimientos para revisar y analizar los registros de eventos, investigar incidentes de seguridad y tomar medidas correctivas adecuadas.

8.2 Copias de Seguridad y Recuperación

Se realizarán copias de seguridad periódicas de los datos críticos de HIGIA BENCHMARKING SL y se almacenarán de manera segura. Se establecerán procedimientos para realizar pruebas de recuperación de datos y garantizar la disponibilidad de los sistemas y la integridad de la información en caso de incidentes o desastres.

8.3 Gestión de Vulnerabilidades

Se implementará un programa de gestión de vulnerabilidades para identificar, evaluar y mitigar las vulnerabilidades de los sistemas y aplicaciones utilizados por HIGIA BENCHMARKING SL. Se establecerán procesos para el seguimiento de las vulnerabilidades conocidas y la aplicación de medidas correctivas oportunas.

9. Continuidad del Negocio

Se establecerá un plan de continuidad del negocio para garantizar la disponibilidad de los servicios críticos de HIGIA BENCHMARKING SL en caso de interrupciones o desastres. El plan incluirá procedimientos de respuesta a incidentes, estrategias de recuperación y procedimientos para la reanudación de las operaciones en un tiempo razonable.

10. Cumplimiento y Auditoría

10.1 Auditorias

Se llevarán a cabo auditorías internas y externas periódicas para evaluar el cumplimiento de esta Política de Seguridad de la Información. Se establecerán procesos para remediar las deficiencias identificadas y se implementarán medidas correctivas y preventivas para mejorar continuamente la seguridad de la información.

10.2 Notificación y Respuesta a Incidentes

HIGIA BENCHMARKING SL implementará un proceso formal para la gestión de incidentes de seguridad de la información. Esto incluirá la notificación oportuna de incidentes, la evaluación de su impacto, la respuesta adecuada para minimizar los efectos negativos y la recuperación de las operaciones normales. También se establecerá un procedimiento para la documentación y el análisis de incidentes, con el fin de identificar áreas de mejora y tomar medidas correctivas.

11. Revisiones y Actualizaciones

La Política de Seguridad de la Información se revisará y actualizará periódicamente para garantizar su vigencia y efectividad. Las actualizaciones se comunicarán a todos los empleados y usuarios relevantes, y se proporcionará la formación necesaria para su cumplimiento.

La Política de Seguridad de la Información será de obligado cumplimiento para todos los empleados, contratistas y terceros que interactúen con los activos de información de HIGIA BENCHMARKING SL. El incumplimiento podrá dar lugar a medidas disciplinarias, legales o contractuales, según corresponda.

Versión 1.2

Barcelona, 19 de junio de 2023