

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN REDUCIDA

Control de versiones

Versión	Autor	Revisión	Aprobado	Fecha	Descripción
1	Resp. SGI	Resp. SGI	Dirección	17/11/2022	Fecha inicial

BICNET es una empresa que se dedica a desarrollar sistemas de información aplicables al entorno hospitalario con la finalidad de optimizar la gestión física y documental del flujo de productos, tanto de suministros como de Farmacia, desde su entrada al almacén general hasta su expedición y consumo, garantizando su trazabilidad y mejorando la gestión de las operaciones fundamentales de todas las áreas del almacén: recepción de mercancía, almacenaje e inventario, preparación de pedidos, expediciones, control de stocks y reaprovisionamiento de subalmacenes.

La Política de Seguridad de BICNET refleja los principios y objetivos en materia de seguridad de la información, cuyos resultados permiten a nuestra empresa alcanzar su propósito de ofrecer servicios relacionados con el diseño, desarrollo y mantenimiento de BICNET.

Mediante la elaboración, comunicación y mantenimiento de esta política, la Dirección de BICNET muestra su compromiso de proteger la confidencialidad de la información con la que opera en la prestación de sus servicios, garantizar su integridad en todos los procesos de tratamiento que lleve a cabo, así como la disponibilidad de los sistemas de información implicados en estos tratamientos.

Para ello, la Dirección ha definido e implantado un Sistema de Gestión de la Seguridad de la Información que permite a la compañía garantizar que los sistemas de información y la información que se crea, recopila, almacena y procesa cumple con:

- La seguridad en la Gestión de los Recursos Humanos, antes, durante y al finalizar el empleo.
- La gestión adecuada de los activos que implique la clasificación de la información y la manipulación de los soportes, y el establecimiento de un robusto control de acceso lógico a sus sistemas y aplicaciones, gestionando los permisos y los privilegios de los usuarios.
- La protección de las instalaciones y del entorno físico, mediante el diseño de áreas de trabajo seguras y la seguridad de los equipos.
- La garantía de la seguridad en las operaciones mediante la protección contra el software malicioso, la realización de copias de seguridad, el establecimiento de registros y su supervisión. el control del software en explotación.
- La gestión de las vulnerabilidades técnicas y la elección de técnicas adecuadas para la auditoría de los Sistemas.
- La seguridad de las comunicaciones, protegiendo las redes y el intercambio de información.
- El aseguramiento de la seguridad en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.
- La realización de un desarrollo seguro de software, separando los entornos de desarrollo y producción, y realizando las pruebas funcionales de aceptación adecuadas
- El control de las relaciones con los proveedores, exigiendo de forma contractual el cumplimiento de las medidas de seguridad pertinentes y unos niveles aceptables en sus servicios.
- La eficacia en la gestión de los incidentes de seguridad, estableciendo los canales adecuados para su notificación, respuesta y aprendizaje oportuno.
- La realización de un plan de continuidad de negocio que proteja la disponibilidad de los servicios durante una crisis o desastre.

- La Identificación y cumplimiento de la normativa aplicable poniendo especial interés en la propiedad intelectual y en la protección de los datos de carácter personal.
- La revisión periódica y mejora continua de nuestro sistema de gestión de la seguridad de la información para garantizar el cumplimiento y eficacia de estos requisitos

Todo el personal de la organización tiene el deber de acatar esta política, para lo cual la Dirección dispone los medios necesarios y recursos suficientes para su cumplimiento, y asume la responsabilidad de comunicar y mantenerla accesible a todas las partes interesadas.

La Dirección
Paterna, 17/11/202