POLITICA DE SEGURIDAD DE LA INFORMACION

FIXMEDICAL SAS BIC

INDICE

INTRODUCCION

La información dentro de la organización es mas que simples palabras escritas, números o imágenes, la información construye la historia de la empresa, marca la trazabilidad de sus procesos y permite evidenciar su actuar. Toda organización recoge, procesa y almacena y transmite la información de diversas maneras, formas que incluyen medios electrónicos, medios físicos, medios verbales, que permiten la transmisión de conocimientos, ideas y marcas, los sistemas, las redes y el personal implicado en la operación, manejo y protección son activos que resultan altamente valiosos para la organización.

Los activos son vulnerables a amenazas que pueden ser deliberadas y/o accidentales, los procesos relacionados, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. La organización debe tener presente que todo su actuar debe estar relacionado con la preservación, mantenimiento y garantía de su información.

La seguridad de la información eficaz reduce los riesgos, protegiendo a la empresa frente a las amenazas y vulnerabilidades. La seguridad de la información se logra con la implementación de una serie de controles, en donde se incluyen políticas, procesos, procedimientos, estructuras organizativas y funciones del aplicativo que se maneje.

Un Sistema de Gestión de la Información SGSI como el que se especifica en la Norma ISO/IEC 27001, brinda herramientas para identificar los riesgos de seguridad de la información con el fin de implantar un conjunto completo de controles de seguridad de la información en el marco de un sistema de gestión coherente.

La identificación de los controles que deberían implantarse requiere una planificación cuidadosa, en donde se evidencie el apoyo y compromiso de todos los empleados de la Organización. En un sentido mas general, una seguridad de la información asegura a la dirección que los activos de la organización están asegurados y protegidos contra daños.

La información tiene un ciclo de vida, que va desde la creación pasando por el almacenamiento, tratamiento, utilización hasta su eventual destrucción. Los sistemas de información tienen ciclos de vida, la seguridad de la información debería ser tenida en cuenta en todas estas etapas.

OBJETIVOS

Establecer e implementar un sistema de gestión de seguridad de la información dentro de la Empresa.

Operar, monitorear, revisar y mantener un Sistema de Seguridad de la Información en la empresa que garantice la información de nuestros clientes, proveedores y funcionarios.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos a la información propiedad de la empresa.

ALCANCE

Esta política cobija el manejo de toda la información de la Empresa, la información relacionada con los clientes, proveedores y funcionarios, garantizando las medidas adecuadas para la protección de la información de acuerdo con su clasificación y análisis de riesgo.

La política de Seguridad de la Información se establece teniendo presente lo estipulado en la Norma ISO 27002.

FIXMEDICAL protege la información y los equipos informáticos teniendo presente:

- Cumplimiento de Normatividad Legal: Fixmedical cumple con lo estipulado en la Ley 23 de 1982, Decreto 1360 de 1989 y la Ley 44 de 1993, evitando en sus equipos todo tipo de copia fraudulenta de software.
- El valor de la información como el activo mas importante de la Empresa.
- La protección de la información, la cual no puede ser usada con fines fraudulentos o para competencia desleal.
- La protección de los equipos, siendo fundamentales para el desarrollo de la operación diaria y como activos de la Empresa.

DECLARACION DE LA POLITICA GENERAL SGSI

La política expresa el compromiso que asume FIXMEDICAL SAS BIC, frente al cumplimiento de los parámetros establecidos para garantizar el manejo acorde y responsable de la información de nuestros funcionarios, clientes y proveedores**.**

Esta política ha sido adoptada por Fixmedical siendo de obligatorio cumplimiento por parte de todos los funcionarios, relacionando aspectos tan importantes como:

- Trabajar con los funcionarios en la implementación de una cultura de cuidado hacia los equipos, el software y la información de la empresa.
- Asumir responsabilidad frente al cuidado de la información de la Empresa, evitando una utilización indebida de la misma.
- Crear conciencia de la importancia del cumplimiento de lo establecido en la política de seguridad de la información establecida por la empresa.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

1. **Objeto y campo de aplicación**

La política de seguridad y privacidad de la información aplica para las áreas de la Organización y se toma como directriz de funcionamiento por parte de la Alta Dirección.

Es obligación de todos los funcionarios su conocimiento y divulgación, así como velar porque la utilización de los equipos de computo, el software y los equipos remotos se haga por el personal autorizado y para el desarrollo de actividades estrictamente laborales.

2. **Referencias Normativas**

La ISO/IEC 27000, es referencia parcial o totalmente en el documento y es indispensable para su aplicación.

3. Términos y Definiciones

En esta política se aplican las definiciones relacionadas en la ISO 27000.

4. Estructura de la Norma ISO 27000

La Norma está compuesta por 18 numerales de control, con sus categorías de seguridad y sus correspondientes controles.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. Política de Datos Personales

Objetivo:

Dar cumplimiento a la Ley 1581 de 2012 “Protección de Datos personales” vigilados por la Superintendencia de Industria y Comercio.

Fixmedical tiene establecida la Política de tratamiento y protección de datos personales Código: P-Q-01. (Anexo No.1).

2. Políticas de Manejo de la Información en Fixmedical

Objetivo:
Establecer los parámetros de actuación, manejo, control y seguimiento del manejo de la información en cada uno de los aspectos relacionados con la Empresa, teniendo como marco de actuación: Funcionarios, software, Hardware, Internet, correo electrónico.

2.1. Manejo de información por parte de los funcionarios

- Cada funcionario tendrá una clave de acceso para sus equipos de computo, cuyo manejo será de su responsabilidad, será única e irrepetible, y será proporcionada por el personal de sistemas de la empresa.
- El área de sistemas realizara auditorias al software verificando inconsistencias que serán responsabilidad del funcionario a quien corresponda el acceso relacionado con la clave.
- En las oficinas se prohíbe comer o consumir líquidos al lado de los equipos de computo.
- Cuando el funcionario termine su jornada laboral o deba ausentarse de su puesto de trabajo, los equipos deben quedar bloqueados, al igual que los escritorios y/o áreas de trabajo deben quedar despejadas, deben quedar libres de documentos sensibles que puedan comprometer los intereses de la empresa.
- El cuidado físico de los equipos de computo le corresponde al usuario a quien se le ha asignado, frente a cualquier movimiento que se requiera del equipo o se necesite deberá notificarlo al departamento de cumplimiento.
- Una vez el funcionario termine su vinculación laboral con Fixmedical, sus claves de acceso serán desactivadas.
- Es obligatorio acceder a los sistemas de información de la empresa solamente por los canales autorizados.
- Esta prohibido descargar en los equipos de computo de la empresa, todo tipo de juegos, plataformas de redes sociales, etc.
- Los procesos implementados por Fixmedical son propiedad de la empresa y se prohíbe totalmente su distribución y/o copia.
- Es responsabilidad de los funcionarios notificar cualquier tipo de situación que ponga en riesgo la integridad, confidencialidad y seguridad de la información de los clientes, proveedores y de los mismos funcionarios.

- Los funcionarios deben asistir de manera obligatoria a las capacitaciones que sobre seguridad informática y política de seguridad de la información programe la empresa.

2.2. Manejo de la información de la empresa

- Cualquier persona teniendo relación con la empresa o no, tiene la responsabilidad de garantizar la reserva de la información a la que haya tenido acceso.
- La información deberá proporcionarse de acuerdo a cargos y responsabilidades, no todos los funcionarios pueden acceder a la información de la empresa.
- La consulta de datos personales solo es manejada por el Departamento de Recursos Humanos.
- La empresa prohíbe enviar información por medios de transmisión como correos electrónicos personales, mensajería instantánea, celulares, sin la autorización del jefe inmediato y/o del Ingeniero de sistemas.
- La empresa prohíbe generar copias, backup sobre bases de datos con información personal, así como información de la empresa catalogada como delicada.
- Para el retiro de información de la empresa, debe hacerse con la autorización por escrito del jefe inmediato y Jefe del Departamento.
- Los funcionarios no están autorizados para destruir o copiar archivos con información de la empresa, que contengan en sus correos electrónicos corporativos.
- La información propiedad de Fixmedical, esta clasificada en CONFIDENCIAL, PRIVADA Y PUBLICA.
- Cada departamento debe generar la clasificación de la información de acuerdo a sus procesos y divulgarlo a la empresa con el apoyo del área de sistemas.
- Fixmedical trabaja en el sistema de Gestión Documental, garantizando así el manejo adecuado de la información, clasificación, archivo y destrucción.
- La información catalogada por la empresa como CONFIDENCIAL debe estar encriptada.
- La información de la empresa solo podrán ser modificados por personal autorizado de acuerdo con los procedimientos establecidos.
- La información de Fixmedical no podrá ser divulgada sin contar con los permisos correspondientes, además, ningún funcionario o contratista puede tomarla una vez se retire de la empresa.
- El área de sistemas de la empresa proporcionara al funcionario las herramientas para el cuidado de la información a su cargo, así como se encargara de conservar esa información para consulta y manejo de la empresa.
- Los equipos de computo, celulares, y otros equipos que se proporcionen al trabajador para el cumplimiento de sus funciones, no deben usarse para actividades personales, el área de sistemas realizara auditorias y controles para garantizar que esta medida se este cumpliendo.

- Los colaboradores del área de sistemas son los únicos autorizados por la empresa para realizar cambios, mejoras, revisiones y demás en los equipos de computo. El funcionario no puede intervenir en la revisión del equipo asignado.
- Cuando un equipo de computo presente fallas el funcionario esta en la obligación de reportarlo a sistemas, no podrá realizar ninguna manipulación que pueda alterar su funcionamiento o presentar daños a la información que maneje.
- Fixmedical cuenta con un inventario de equipos actualizado, donde se especifica el funcionario responsable de cada equipo, las características del equipo, la configuración, la ubicación, el numero asignado.
- Los equipos portátiles de computación que contengan información sensible deben utilizar software de encryption.
- Para el manejo de equipos de computo portátiles, el funcionario debe diligenciar acta de entrega de equipo donde se especifican las condiciones de manejo, la responsabilidad sobre el uso y la conservación del mismo así como las directrices de actuación establecidas frente a perdida o robo.
- Fixmedical prohíbe el uso de unidades personales para grabar información, de necesitarse por parte del funcionario debe ser solicitado al área de sistemas.
- El uso de dispositivos de almacenamiento extraíble esta prohibido.
- Se prohíbe sacar equipos de la empresa sin previa autorización.
  Política de Dispositivos Móviles P-DM-G-001 /Anexo 2 Política de uso de celulares P-AD-02 / Anexo 3

2.3. Manejo de la información a través de internet

- Cada estación de trabajo tendrá acceso a internet, tendrá limitado el acceso a redes sociales, plataformas de juego y demás sitios de internet que no tienen relación con su trabajo.
- Los funcionarios deben manejar de forma responsable el acceso a internet, evitando a toda costa el ingreso de virus que puedan alterar el funcionamiento de los equipos, del software y demás canales de comunicación de la empresa.
- Apropiarse de material consultado en internet que pueda violar la ley de derechos de autor.
- Durante la jornada laboral ingresar a sitios que no tengan relación con las funciones de su trabajo, así como visitar sitios de chat que no tengan que ver con sus funciones y/o con el objetivo de la empresa.

2.4. Manejo de la información a través de correo electrónico

- A cada funcionario se le asigna una cuenta de correo electrónico con un usuario y clave que serán personales e intransferibles.
- El funcionario debe abstenerse de enviar mensajes abusivos, groseros, o emitiendo conceptos políticos, etc. a través del correo institucional.

- Esta estrictamente prohibido el envío de cadenas, memes y material que no tenga relación con sus funciones y/o cargo.
- Fixmedical no autoriza el uso de cuentas personales para el envío de información relacionada con la empresa.
- El tamaño de las cuentas de usuarios y los archivos adjuntos esta asignado de acuerdo a las responsabilidades correspondientes al cargo.

2.5. Manejo de la información con los proveedores y clientes

Todos los proveedores y clientes de Fixmedical tendrán conocimiento de la Política de manejo de la seguridad de la información, así como Fixmedical solicitara a proveedores y clientes su política de manejo de la información, esto para tener claridad sobre el actuar con la información suministrada por la empres.
Los proveedores y Clientes están en la obligación de presentar su Política de Seguridad y Privacidad de la Información.

Los proveedores solo tendrán acceso a los recursos de red, aplicaciones e información que sean necesarios para el correcto desempeño del servicio contratado.

Todo tipo de contrato que se genere con Fixmedical y un tercero, y que implique manejo de información, debe incluir controles de seguridad tecnológica.

El acceso a la información esta restringida por parte de Fixmedical en relación con las condiciones establecidas en el contrato.

El proveedor esta obligado a notificar cualquier incidente de seguridad que se produzca en la prestación del servicio.

El proveedor garantizara el cumplimiento de lo establecido en la Ley 1581 "**Protección de datos personales".** En función del servicio contratado Fixmedical realizara comprobaciones de cumplimiento técnico sobre los recursos de tratamiento de la información.

3. Políticas de seguridad de los Recursos Humanos

Fixmedical, realiza verificación de referencias personales y familiares de los candidatos, sin dejar registro del concepto emitido, se relaciona en el formato de selección, especificando contacto con la persona, sus datos y fecha y hora de contacto. La verificación de las referencias laborales se realiza con la autorización del candidato.

3.1. Términos y condiciones del empleo

Fixmedical contempla en su contrato laboral como parte integrante del mismo el Acuerdo de confidencialidad que reglamenta el manejo de la información de entre ambas partes.

3.2. Durante la ejecución del empleo

Fixmedical mediante la capacitación asegura de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

3.3. Responsabilidades de la Dirección

Fixmedical genera documento anexo al contrato comprometiendo al funcionario con el cumplimiento de la Política de Seguridad y Privacidad de la Información.

3.4. **Toma de conciencia, educación y formación en la seguridad de la información**.

Fixmedical, incluye dentro del proceso de induccion y entrenamiento capacitación en el cumplimiento de la política de Seguridad y Privacidad de la Información. De forma regular incluye en su programa de capacitación y actualización la política para funcionarios que lleven tiempo dentro de la Organización.

3.5. Proceso Disciplinario

Fixmedical, incluye en su Reglamento Interno de Trabajo como falta grave el incumplimiento de la Política de Seguridad y Privacidad de la Información. Recursos Humanos se encarga de levantar el correspondiente proceso disciplinario ante el incumplimiento a cualquiera de los apartes de la política.

4. Gestión de Activos

Responsabilidad por los activos

Fixmedical tiene definida una política de manejo de activos, incluyendo cargos, responsabilidades en los activos, proceso de entrega de activos una vez se vincula a la organización el trabajador y entrega de activos una vez se retira de la organización. Fixmedical, es propietaria como Organización de cada uno de los activos que conforman la empresa. El registro de los activos se encuentra en documento: Inventario de Activos Fixmedical.

4.1. **Devolución de activos**

Fixmedical, en su proceso de retiro incluye de acuerdo con la relación de activos asignada a cada cargo la entrega de los mismos, verificando el estado de su entrega. Con respecto al manejo de la información contenida en correos, WhatsApp, drive, retorna a la empresa, Fixmedical procede al cancelamiento de claves que permitan acceso a la información.

4.2. Política de escritorio y pantalla limpios

Fixmedical, adopta la política de escritorio y pantalla limpios, acogiéndose al proceso que se establece desde la metodología 5s y construyendo e implementando cronograma de actualización de la pantalla, de la información, etc.

5. SEGURIDAD DE LAS OPERACIONES

Fixmedical establece la política de protección de antivirus, para garantizar el correcto funcionamiento de sus equipos.

Política de Protección antivirus P-G-RH-01
Política de Gestión de Parches P-G-SI-01

Copias de respaldo
Fixmedical, por medio de la empresa Red Expertos y el área de sistemas, se realizan tres copias de seguridad al día, mediante la nube, una copia de seguridad al medio día, una copia de seguridad a las 8 de la noche, esta copia es guardada en un disco externo que esta bajo el cuidado del responsable de Sistemas Informáticos en la Empresa.

FUNCIONES DE CONTROL Y RESPONSABILIDADES EN CUMPLIMIENTO DE LA POLITICA

1. Definir, implementar, políticas, normas, estándares y procedimientos necesarios para proteger la confidencialidad de la información de Fixmedical SAS BIC.
2. Supervisar que las excepciones a las políticas de seguridad estén autorizadas únicamente por la Alta Dirección dejando constancia de los riesgos que en forma consiente se estén asumiendo.
3. Implementar un plan de seguridad que permita controlar la información estratégica, teniendo en cuenta criterios de confidencialidad, integridad, disponibilidad de la información.
4. Establecer las directrices básicas de seguridad informática para el manejo del harward y el software.
5. Implementar mecanismos de monitoreo con el fin de detectar procedimientos inseguros para los sistemas operacionales, datos y redes.
6. Sistemas Informáticos puede acceder a cualquier equipo de computo para realizar su supervisión.
7. Revisar de manera continua las políticas de seguridad informática.
8. Documentar los incidentes de seguridad.
9. Actualizar permanentemente el reglamento para uso de red y procurar su cumplimiento.

LOS PROVEEDORES

1. Los proveedores deben notificar a FIXMEDICAL cualquier sospecha que se tenga sobre el uso indebido de la base de datos y/o aplicativos que pongan en riesgo la seguridad informática.
2. El proveedor únicamente tendrá acceso a aquellos recursos de red, aplicaciones e información que sean necesarios dentro del desarrollo del contrato realizado.
3. Los contratos con terceros que impliquen acceder, procesar, comunicar la información de Fixmedical deben incluir controles de seguridad tecnológica requeridos para la prestación del servicio.
4. Todo cambio en la prestación del servicio y que signifique un cambio en las personas que participan en el mismo, deberá será comunicado a Fixmedical oportunamente.
5. El acceso a la información será restringido en función a la necesidad de conocer los servicios contratados con cada proveedor.

SANCIONES

1. Cualquier violación a las políticas de seguridad, deberá ser sancionada de acuerdo a lo estipulado en el Reglamento Interno Laboral.
2. Las sanciones van desde una llamada de atención hasta la suspensión, dependiendo de la gravedad de la falta.
3. Corresponderá a RRHH junto con Sistemas informáticos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática. **Esta política se revisara y renovara anualmente.**

Control de Cambios

Fecha	Cambio	Versión
01/12/23	Lanzamiento	Versión 01