**Política General de Seguridad de la Información**

|  |  |
| --- | --- |
|  | Versión: 1.0 |
| Autores: |
| Fecha:dd/mm/aa |

1. Resumen

En la presente política se describe de forma general los lineamientos de seguridad en los que se debe manejar la empresa, tratamiento de los activos según su categoría, los roles y responsabilidades de la seguridad y las posibles sanciones a las que están expuestos por el incumplimiento de estas políticas de seguridad.

1. Objetivo

Establecer lineamientos para la gestión de la seguridad de la información que permita la protección adecuada de los activos de información frente a las amenazas a las cuales se encuentra expuesta la organización, tanto internas como externas, deliberadas o accidentales con la finalidad de asegurar la Integridad, disponibilidad y confidencialidad de la información.

1. Alcance

La siguiente política de seguridad de la información es aplicable a toda la organización, empleados, entidades y profesionales contratados bajo otras modalidades. Este documento debe ser revisado y actualizado periódicamente según se crea conveniente respecto a cambios significativos dentro de la organización como el uso de nuevas tecnologías, nuevos servicios, cambios en la infraestructura, entre otros. A su vez, se toman consideraciones para el cumplimiento de las leyes de protección de datos, y regulatorios que aplican a las entidades de salud.

1. Generalidades

• mediplus reconoce la importancia de la información y de los sistemas de información, así como la necesidad disminuir las vulnerabi1idades y protegerlas de las amenazas a los que se encuentran expuestos ya que puede constituir un peligro a la continuidad del negocio o daños muy importantes si se produjera una pérdida irreversible de datos. A su vez los establecidos en la legislación de la seguridad de los datos personales y en defensa de los intereses de los clientes, empleados y otros posibles afectados.

• Los accesos y usos de la información, estarán alineadas a las normativas internas, reglas, estándares y procedimientos de mediplus.

• Los empleados deben tener conocimiento de las políticas, normas, reglas, estándares y procedimientos y de igual manera, deberán conocer los documentos de seguridad que hagan referencia a datos de carácter personal.

• Se deberá contar con una adecuada segregación de funciones y revisión de las operaciones o transacciones que se realicen que permitan la identificación de la persona, cuando lo hizo y donde.

• Para la prevención de fraudes, delitos, errores u omisiones, se fomentará la difusión de la información y se promoverá una cultura de seguridad de información entre los colaboradores.

• Cada rol de usuario solo podrá realizar las tareas y acceder a datos necesarios y previamente autorizados.

• Se establecerán los medios necesarios y adecuados para proteger a las personas, datos, software, hardware, documentación y en general cualquier activo de seguridad de la información de mediplus.

• En caso de baja de un empleado se deberá entregar llaves, tarjetas de acceso, usuarios, equipos o cualquier tipo de información entregados o recopilados en sus funciones realizadas en mediplus. Si hubiera algún indicio de que no se devolvió toda la información, se analizará si ha podido realizar copias digitales o físicas, o haber introducido datos erróneos a la información de la empresa.

• La información debe clasificarse en alguno de los siguientes niveles:

• Activo Libre, se puede difundir y es de dominio público.

• Activo Restringido, solo puede debe ser de uso interno. Si se filtra, no ocasionar(a no ocasionaría un riesgo.

• Activo Protegido, se debe tener controles para el acceso. Sí se llega a filtrar, ocasionaría un riesgo moderado al negocio.

• Activo Confidencial, información sensible y no se puede difundir bajo ningún concepto. Su filtración ocasionaría un riesgo crítico para el negocio.

• Las zonas restringidas de la mediplus deben contar con controles para impedir el daño o pérdida de información.

• Los puertos para medios removibles serán desactivados en todas las computadoras de la clínica. Si se requiere el uso del algún medio removible, debe justificarse a la administración.

• Se debe tener conocimiento y comunicar las políticas específicas de seguridad a todos los trabajadores de la clínica. Ante cualquier actualización, también debe ser comunicado especificando los cambios realizados.

• Se debe tener un proceso periódico para el inventariado de los activos de información de la empresa, según crea conveniente la administración de la mediplus.

• La política general de seguridad de la información y las políticas específicas, deben ser revisadas al menos 1 vez al año para su actualización.

1. Responsabilidades

La responsabilidad de la seguridad de la información es de la gerencia general y el área de administración según sea el caso. Esto no niega que cada empleado deba asumir su responsabilidad respecto a los medios que utiliza, según los puntos que se indican las políticas, sus normas y procedimientos.

1. Sanciones

La violación de un control de seguridad o de la presente política justifica la aplicación de sanciones disciplinarias de acuerdo al reglamento interno de trabajo de mediplus, las cuales serán aplicadas teniendo en consideración lo siguiente:

Naturaleza y gravedad de la falta, antecedentes del empleado, reincidencias y circunstancias en que se cometió la falta. La administración de mediplus es la encargada de determinar la gravedad de las faltas.

De acuerdo a la gravedad de la falta cometida, la gerencia podrá aplicar cualquiera de las siguientes sanciones:

* Amonestación verbal
* Amonestación por escrito
* Suspensión de labores
* Despido

Las amonestaciones verbales se impondrán a los trabajadores que cometan faltas por primera vez y que sean faltas leves.

Las amonestaciones por escrito se impondrá a los trabajadores que sean reincidentes en faltas leves o si cometen f faltas que se considere que debe haber una amonestación más que verbal.

La suspensión de labores se impondrá a los trabajadores que hayan sido amonestados de manera reiterativa tanto verbal como escrita o que cometan faltas que no constituyan causal de despido.

Las sanciones no necesariamente se impondrán de forma progresiva. La gravedad de la falta determinará la sanción a imponerse.

1. Políticas Especificas

Las políticas específicas de seguridad de la información deben estar alineadas y soportadas por la política general de seguridad. Estas políticas son las siguientes:

* Política de Gestión de Contraseñas
* Política de Escritorio Limpio
* Política de Gestión de Accesos
* Política de Gestión de Incidentes
* Política de Gestión de Copias de Respaldo
* Política de Gestión de Activos