POLÍTICAS DE SEGURIDAD y MANEJO DE LA INFORMACIÓN

FunPaz IPS CLINICA DE SALUD MENTAL

Área de Sistemas

2023

Elaboró: oficina Área de sistemas	Versión 2.0.0.
Aprobó:	Fecha de Modificación: Julio de 2023

FunPaz I.P.S
Clínica de Salud Mental

INDICE **Pág.**

1. INTRODUCCIÓN

La clínica de salud mental FunPaz IPS, viene adelantando unos importantes procesos de adaptaciones Metodológicos y organizacionales al interior de la clínica, es por esto que, se ve la necesidad latente de cuidar y proteger la información como el mayor activo documental que posee la institución.

También se dice que, los niveles de seguridad con los que cuenta hoy en día las tecnologías de la información son cada vez más de mayor complejidad, atribuidos a la forma como viene creciendo y desarrollándose el ciberespacio en estas últimas décadas. La protección de información y bloqueo de intrusos, son tan solo ejemplos de los objetivos a lograr para que la infraestructura informática de una organización sea segura.

La posibilidad de expandir la cobertura de servicios, de interconectar bases de datos y de acercar a los usuarios separados por grandes distancias, ha llevado a la aparición de nuevas amenazas en los sistemas computarizados, si crece la cobertura, crece la vulnerabilidad.

Hoy en día, muchas de las organizaciones públicas y privadas, ya sean de ámbito local nacional o internacional, desarrollan políticas de seguridad al interior de su organización, creando una cultura entre sus miembros para el buen uso y adecuado manejo de la tecnología y por ende de la información.

Las políticas de seguridad informática surgen como una herramienta organizacional necesaria para concientizar a cada uno de los integrantes de una empresa sobre la importancia, la sensibilidad de la información y la necesidad de su conservación con el mínimo de riesgo y un alto grado de seguridad que favorezca el desarrollo de la organización, garantice su óptimo funcionamiento y el buen uso de los equipos y recuperación de la información en el menor tiempo posible en caso de incidentes o eventos catastróficos.

2. JUSTIFICACIÓN

La masiva utilización de recursos informáticos (Computadores, impresoras, redes de datos, etc.) Como medio para almacenar, transferir y procesar información, se ha incrementado desmedidamente en las últimas décadas, al punto de convertirse en un elemento esencial para el funcionamiento de la sociedad y de las diferentes Empresas sean de carácter gubernamental o No Gubernamental.

En consecuencia, la información, y por consiguiente los recursos mencionados anteriormente, se han convertido en un activo de altísimo valor, de tal forma que, la clínica de salud mental FunPaz IPS no puede ser ajeno a esta situación y por lo tanto, se hace necesario proteger, asegurar y administrar la información para garantizar su integridad, confidencialidad y disponibilidad, de conformidad con lo establecido por la normatividad.

En los últimos años se ha incrementado el uso de aplicaciones electrónicas que comprenden: correo electrónico, internet, transacciones, firmas y certificados digitales, comunicaciones seguras, entre otras. Por tal motivo, los requerimientos de seguridad son cada vez mayores.

Es evidente que la vulnerabilidad de los sistemas crece al mismo ritmo y es necesario que las medidas de seguridad y protección sean cada vez más eficientes y menos fáciles de burlar por personas dedicadas al hacking, virus informáticos, software espía y demás ataques que traten de afectar la información de las empresas. Cada día las empresas de nuestro país y de nuestra región tienen un riesgo mayor de sufrir ataques por hackers, incluso algunas ya se han visto afectadas por problemas de virus, caída de servidores y pérdida de valiosa información. Las amenazas están en todo tipo de entidades, y pueden ser externas

o internas, entre ellas tenemos: Uso indiscriminado de la Internet, mala práctica de los usuarios, descuido en la manipulación de los equipos y el desconocimiento de conceptos básicos de manejo de dispositivos informáticos

Según los anteriormente expuesto en el texto, se requiere que la clínica de salud mental FunPaz IPS, en su función de ofrecer recursos informáticos, seguros, estables y confiables, decide elaborar un Manual de Políticas de Seguridad que compile las medidas tomadas en los últimos meses, y con el fin de poder garantizar, el cumplimiento de las políticas que le asegurarán a la entidad una protección continua tanto para los activos tangibles como para los intangibles.

3. OBJETIVOS

3.1 OBJETIVO GENERAL:

✔ Elaborar un Manual de Políticas de Seguridad de la información para la Clínica de salud mental FunPaz IPS, que cree una cultura organizacional de buenas prácticas y manejo en el aspecto computacional y lo concerniente a la información.

3.2 OBJETIVOS ESPECÍFICOS:

✔ Establecer parámetros de cuidado de equipos, periféricos y demás dispositivos físicos y lógicos

✔ Fortalecer la protección física y lógica de los activos informáticos de la entidad.

✔ Sensibilizar a cada uno de los empleados de la clínica, acerca de la importancia y la necesidad de poner en práctica las políticas.

✔ Implementar mecanismos de protección a partir de la toma de precauciones, básicas pero muy necesarias en el instante que cada uno de los miembros decida hacer uso de las redes ya sea el internet o la intranet.

✔ Diseñar, Reglamentar, controlar, la instalación de todo tipo de hardware y Software, por parte de los empleados y contratistas de la clínica FunPaz IPS.

✔ Documentar por escrito las políticas de seguridad de la información para la clínica de salud mental FunPaz IPS, Estableciendo parámetros claros acerca del buen uso de los elementos tecnológicos como su información.

4. ORGANIGRAMA

5. GLOSARIO

Para efectos del presente documento se entiende por:

Red: Una red es una estructura que dispone de un patrón que la caracteriza. La noción de informática, por su parte, hace referencia a los saberes de la ciencia que posibilitan el tratamiento de datos de manera autorizada automatizada a través de computadoras

Internet: Se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios

Intranet: Red informática interna de una empresa u organismo, basada en los estándares de Internet, en la que las computadoras están conectadas a uno o varios servidores web.

LAN: Se conoce como red a la estructura que tiene un patrón característico, el cual permite vincular sus diversos componentes. A partir de este significado, puede hablarse de diferentes tipos de redes.

Datos: Cifra, letra o palabra que se suministra a la computadora como entrada y la máquina almacena en un determinado formato.

Administrador del sistema: Un administrador de sistemas es la persona que tiene la responsabilidad de implementar, configurar, mantener, monitorizar, documentar y asegurar el correcto funcionamiento de un sistema informático o algún aspecto de este.

Seguridad: Podemos definir que es la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático

Computador: Máquina electrónica capaz de almacenar información y tratarla automáticamente mediante operaciones matemáticas y lógicas controladas por programas informáticos

Hacker: Persona con grandes conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos.

Contraseña: Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

Backup: Se define como «copia de seguridad» y permite guardar y almacenar los ficheros, archivos y aplicaciones disponibles en un soporte informático como un teléfono móvil o un ordenador y tiene el objetivo de permitir la recuperación de estos datos a posteriori.

Dirección Ip: La idea de dirección puede referirse a un domicilio. En el caso específico de la informática, se trata de una expresión compuesta por letras y/o números que alude a una localización en la memoria de un equipo informático

Software: es un término informático que hace referencia a un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático**.**

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Servidor: Un servidor es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Rac: Es un término inglés que se emplea para nombrar a la estructura que permite sostener o albergar un dispositivo tecnológico. Se trata de un armazón metálico que, de acuerdo a sus características, sirve para alojar una computadora

Cableado estructurado: consiste en el tendido de cables en el interior de un edificio, con el propósito de implantar en un futuro una red de área local. Suele tratarse de cable de par trenzado de cobre UTP/STP, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

Conmutador: Dispositivo automático empleado en radar para evitar que la energía emitida alcance al receptor, pero permitiendo que la energía recibida llegue sin pérdidas apreciables.

Elementos de tecnología: La tecnología se define usualmente como el conjunto de herramientas hechas por el hombre, como los medios eficientes para un fin, o como el conjunto de artefactos materiales

Usuario: Se refiere a la persona que utiliza un producto o servicio de forma habitual

Contraseña o Password: Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso

Megabyte MB: es el nombre de una unidad de información equivalente a un millón de bytes aproximadamente

Administrador de correo: Un Gestor de correos electrónicos es un programa que nos va a permitir, como su nombre indica, gestionar o trabajar con diferentes cuentas de correo electrónico a la vez

Sistema operativo: Un sistema operativo es un conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los diferentes periféricos o recursos de nuestra computadora

SPAM: Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

Soporte básico: La noción de soporte se utiliza para nombrar a algo que brinda un respaldo, que puede ser físico o simbólico. Lo técnico, por otra parte, se asocia a aquello que se aplica en la ciencia o una disciplina artística

Mantenimiento preventivo: En el área de informática, el mantenimiento preventivo consiste en la revisión en el software y hardware de la PC u ordenador lo que permite al usuario poseer un equipo fiable para intercambiar información a una máxima velocidad con respecto a la configuración del sistema

Mantenimiento Correctivo: Como mantenimiento correctivo se denomina aquel que se realiza con la finalidad de reparar fallos o defectos que se presenten en equipos y maquinarias.

Virus informático: Un virus o virus informático es un software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo.

Firewall: Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Un firewall puede ser hardware, software o ambos

Crack: Un crack informático es un parche creado sin autorización del desarrollador del programa al que modifica cuya finalidad es la de modificar el comportamiento del software original.

FTP: Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.

Router: Un rúter, enrutador, (del inglés router) o encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Swich: El switch es un dispositivo que se utiliza para conectar equipos en red, formando una red de área local (LAN) y se encargan de la interconexión de dispositivos cableados, que siguen las especificaciones técnicas del estándar Ethernet. Switches; se encargan de la interconexión de equipos dentro de una misma red.

6. ALCANCE

La aplicación del Manual de Políticas de Seguridad Informática, de la clínica de salud mental FunPaz IPS, va dirigido a todos los funcionarios, contratistas, de planta, asistenciales y administrativos que hagan uso de las distintas herramientas Tecnológicas y de informática y que se encuentren utilizando la red de la institución. La política de seguridad y manejo de la información que se vaya a implementar, es necesario tener un alto sentido de pertenencia por cada uno de los funcionarios de la clínica, el compromiso será grande a la hora de poder detectar cualquier falla en nuestro día a día.

7. VIGENCIA

Este documento regirá a partir del momento en que mediante Acto Administrativo sea aprobado por la Gerencia y su junta directiva, como documento técnico de seguridad informática, el cual deberá ser revisado y actualizado conforme a las exigencias y necesidades de la clínica de salud mental FunPaz IPS.

8. RIESGOS INFORMATICOS

La ISO 27001 (Organización Internacional de Estandarización) define el riesgo informático como: "**La posibilidad que una amenaza se materialice, utilizando**

vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños."

En una entidad, los riesgos informáticos, son latentes día a día y pueden afectar gravemente la seguridad y la estabilidad de los sistemas de información, estos pueden presentarse en diversas áreas como son los riesgos externos y los riesgos internos.

8.1 GRAFICA (1).

Método de Evaluación y Tratamiento del Riesgo

9. QUÉ SON POLÍTICAS DE SEGURIDAD?

Según diferentes conceptos y autores, se puede decir que, la seguridad informática es una serie de normas y lineamientos precisos que consisten en garantizar el valor significativo de la información de la institución, es poder minimizar los riesgos que

puedan llegar a ingerir de manera traumática el normal desarrollo del día a día. Una verdadera política de seguridad se define como el control garantizado que se va a implementar, es una serie de direccionamientos e instructivo de la información y que se debe hacer cumplir.

9.1 CLASIFICACIÓN DE POLÍTICAS DE SEGURIDAD

Para efectos de la clasificación del grupo de políticas de seguridad y de la información en la clínica de salud mental FunPaz IPS, se crearon los siguientes grupos nominales que se pensaría que son los de mayor relevancia e idoneidad:

- ✔ **Equipos**: Todo lo relacionado con el hardware, su uso y cuidado.
- ✔ **Usuarios**: Concerniente a las personas, funcionarios, administrativos que utilizan los recursos informáticos de la institución.
- ✔ **Software**: los recursos lógicos tales como programas, aplicativos entre otros.
- ✔ **Redes e Internet**: las medidas correctivas que se deben tomar en el momento de hacer uso de los recursos de telecomunicaciones.
- ✔ **Datos e Información**: Políticas que regulan la manipulación, transporte y almacenamiento de la información de la institución.
- ✔ **Administración de seguridad informática**: Establece la forma en que la Oficina de Sistemas de Información gestiona la seguridad de la infraestructura informática de la clínica de salud mental FunPaz IPS.

10. POLÍTICA DE SEGURIDAD DE SOFTWARE - FUNPAZ IPS

1. El Área de Sistemas de la clínica de salud mental FunPaz IPS, es la única responsable de la instalación de software informático y de telecomunicaciones.

2. En los equipos de cómputo de la clínica de salud mental FunPaz IPS, no se permite la instalación de software que no cuente con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de “Cracks”, “Keygens” y demás aplicativos.

3. Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la clínica de salud mental FunPaz IPS**.**

4. Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

5. Las medidas de protección lógica (a nivel de software) son responsabilidad del personal de sistemas de información y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad a la oficina de Sistemas de Información.

6. La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por la oficina de Sistemas de Información y a la disponibilidad presupuestal con la que se cuente.

7. Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente a la Oficina de sistemas sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardadas en sitios debidamente adecuados para tal fin.

11. PROTECCIÓN DE DATOS EN CLÍNICAS Y HOSPITALES- POLÍTICAS DE SEGURIDAD INFORMÁTICA

Cuando hablamos de protección de datos a nivel clínico y hospitalario, estas se convierten en un punto neurálgico para la protección de su información y su data, el estado de salud y la información personal de cada paciente hace que sea sensible a pretender ser penetrado muchas veces con mala intención. El tener un número significativo de funcionarios ya sean administrativos, asistenciales entre otros, manipulando la información de cada uno de los pacientes, hace que exista una gran fuga de información personal única e intransferible. La protección de datos personales en Colombia es un hecho, hoy en día un usuario puede saber qué datos digitales manejan las organizaciones y habilitar o deshabilitar su uso para fines comerciales, de investigación o de publicación. Adicional a esto, **Ley 1581 de 2012, en el Título 3**, posiciona los datos relacionados a la salud como un tipo de dato destacado y que merece especial protección.

Para ayudar a concentrar los esfuerzos, aquí hay consejos de seguridad informática que pueden ser aplicados para la protección de información en clínicas y hospitales

- ✔ Establecer una cultura de seguridad
- ✔ Controle el acceso a la información protegida
- ✔ Proteger los dispositivos móviles
- ✔ Mantener una buena higiene cibernética
- ✔ Configurar correctamente un cortafuegos o “firewall”
- ✔ Instalar y mantener un software antivirus
- ✔ Copia de seguridad de los datos
- ✔ Use contraseñas seguras y cámbielas regularmente
- ✔ Control de acceso físico

12. NORMATIVIDAD

FUNPAZ IPS CLINICA DE SALUD MENTAL

POLÍTICA DE PROTECCIÓN DE DATOS NORMATIVIDAD

12.1 INTRODUCCIÓN

FUNPAZ IPS CLINICA DE SALUD MENTAL, con domicilio en la ciudad de Manizales, NIT 900.413.177– 2, en su calidad de responsable del tratamiento, por medio del presente Manual Interno de Políticas y Procedimientos sobre Tratamiento de Datos Personales (en adelante el "Manual") da cumplimiento a las disposiciones de la Ley 1581 de 2012 y el Decreto 1377 de 2013 y demás normas aplicables.

12.2 GENERALIDADES

La Ley 1581 de 2012 estableció las reglas y principios aplicables para la protección y manejo de los datos personales y el Decreto 1377 de 2013 reglamentó su aplicación.

El objetivo de la Ley es desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar información de bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política (derecho a la intimidad personal, familiar y al buen nombre), así coma el derecho a la información consagrado en el artículo 20 de la misma.

Se exceptúan de la aplicación de la Ley 1581 de 2012 y del Decreto 1377 de 2013, lo relativo a las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico, es decir, las actividades comprendidas en el marco de la vida privada o familiar de las personas naturales.

La entidad encargada de garantizar el cumplimiento de las disposiciones sobre datos personales es la Superintendencia de Industria y Comercio (SIC).

12.3 DEFINICIONES

FUNPAZ IPS CLINICA DE SALUD MENTAL, tiene en cuenta las siguientes definiciones en el tratamiento de datos personales:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **Base de Datos**: Conjunto organizado de datos personales que sea objeto de Tratamiento.

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y su tratamiento.

- **Titular:** Persona natural o jurídica cuyos datos sean objeto de Tratamiento.

- **Tratamiento**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Aviso de privacidad**: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que te serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos

- **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o el Encargado del Tratamiento de datos personales, ubicado en Colombia, envía

información de los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

- **Transmisión**: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable

12.4 PRINCIPIOS

FUNPAZ IPS CLINICA DE SALUD MENTAL, aplica los siguientes principios en el tratamiento de datos personales:

- **Principio de legalidad:** El tratamiento de datos personales se sujetará a lo establecido en las disposiciones normativas sobre la materia.

- **Principio de finalidad**: El tratamiento de datos personales a los que tenga acceso y sean recolectados, almacenados, depurados, analizados, actualizados por FUNPAZ IPS CLINICA DE SALUD MENTAL, y/o por los encargados, atenderá la finalidad legítima informada al Titular de los datos.

- **Principio de libertad:** El tratamiento de los datos se llevará cabo con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal, estatutario, o judicial que releve el consentimiento.

- **Principio de veracidad o calidad**: La información sujeta a tratamiento será veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- **Principio de transparencia:** El tratamiento de datos personales garantizará el derecho del Titular a obtener de FUN PAZ IPS CLINICA DE SALUD MENTAL, en cualquier momento y sin restricciones, información acerca de los datos de su interés.

- **Principio de acceso y circulación restringida:** Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los Titulares o terceros autorizados.

- **Principio de seguridad:** La información sujeta a tratamiento por FUNPAZ IPS CLINICA DE SALUD MENTAL, será manejada con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información inclusive después de finalizada su relación con algunas de las labores que comprende el tratamiento.

12.5 AUTORIZACIÓN DEL TITULAR

En el Tratamiento de datos personales se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.
Para ello se establecen mecanismos tendientes a obtener la autorización del Titular, a través de medios técnicos que faciliten la manifestación automatizada tales como

escrito, de forma oral o mediante conductas inequívocas del Titular que permiten concluir que otorgó la autorización. Sin embargo, en ningún caso el silencio puede ser asimilado a una conducta inequívoca.

La autorización del Titular no es necesaria cuando se trata de: información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; de datos de naturaleza pública; de casos de urgencia médica o sanitaria; de tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; o de datos relacionados con el Registro Civil de las Personas.

Para solicitar la autorización del Titular, FUNPAZ IPS CLINICA DE SALUD MENTAL, como Responsable del Tratamiento adopta procedimientos para solicitar dicha autorización, a más tardar en el momento de la recolección de los datos. En caso de cambiar la finalidad del Tratamiento solicitará una nueva autorización del Titular.

Para efectos de dar cumplimiento a las obligaciones inherentes y necesarias a los servicios y productos que ofrecemos y que son contratados, es necesario obtener mínimo la siguiente información del Titular: nombres, apellidos, razón social, documento de identificación, dirección, correo electrónico y teléfonos de contactos. Una vez obtenida la autorización del Titular para recolectar, almacenar, depurar, usar, analizar, circular, actualizar y cruzar con información propia o de terceros, a través de cualquier medio y en forma directa o a través de encargados del tratamiento para realizar actividades de mercadeo, promoción y/o publicidad propia, contratación se servicios, facturación, gestión de cobranza, verificaciones y consultas, así como cualquier otra relacionada con nuestros servicios, actuales y futuros para el cumplimiento de las obligaciones contractuales y de nuestro objeto social, el Titular reconoce que sus datos personales serán recogidos y utilizados para las finalidades contenidas en el presente Manual.

La autorización del Titular constituye una declaración de reconocimiento sobre la persona o entidad que recopila la información, la clase y contenido de la información que se recopila, la finalidad para la cual se recopila y la forma cómo puede ejercer sus derechos, por cuanto la facultad de decisión del Titular sobre sus datos personales implica el reconocimiento que su información es objeto de Tratamiento, conforme a las disposiciones legales y a lo establecido en este Manual. **FUNPAZ IPS CLINICA DE SALUD MENTAL**, adopta las medidas que considere necesarias para mantener y garantizar el registro de cuándo y cómo obtuvo la autorización del Titular de los datos personales

12.6 DERECHOS DEL TITULAR

Conforme a las disposiciones normativas sobre datos personales el Titular tiene los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento.
- Ser informado, previa solicitud, respecto del uso que se les dará a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en las normas sobre datos personales.
- Solicitar la supresión de los datos personales.
- Revocar la autorización mediante la presentación de una solicitud y/o reclamo. Esta no procede cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.
- Solicitar a la SIC que ordene la revocatoria de la autorización y/o la supresión de los datos.

12.7 PROCEDIMIENTO PARA EFECTUAR CONSULTAS

Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquiera de nuestras bases de datos.

FUNPAZ IPS CLINICA DE SALUD MENTAL, dará trámite a las solicitudes efectuadas por los Titulares en relación con el tratamiento de sus datos personales. Para tal efecto, es necesario que el Titular o su representante legal se identifiquen y haga una descripción clara, precisa y detallada de los datos respecto de los cuales fundan su solicitud o busca ejercer alguno de sus derechos, con el fin de poder garantizar una respuesta oportuna y efectiva.

En el caso de consultas y reclamos, **FUNPAZ IPS CLINICA DE SALUD MENTAL**, dará respuesta a los peticionarios dentro del término establecido en la ley 1581 de 2012, esto es en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Con el fin de garantizar el derecho de consulta de los Titulares de la información, **FUNPAZ IPS CLINICA DE SALUD MENTAL**, pone a su disposición mecanismos idóneos de consulta, telefónicos y electrónicos.

12.8 PROCEDIMIENTO PARA EFECTUAR RECLAMOS

El Titular que considere que la información contenida en nuestra base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo a través de nuestras líneas telefónicas antes señaladas, o nuestro correo electrónico, el cual será tramitado bajo las siguientes reglas:

- El reclamo se formulará mediante solicitud dirigida a FUNPAZ IPS CLINICA DE SALUD MENTAL, con la debida identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

- En caso de que quien reciba el reclamo no sea competente para resolverlo, se dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informaremos de la situación al interesado.

- Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

12.9 REQUISITO DE PROCEDIBILIDAD

Es importante que el Titular o causahabiente tenga en cuenta que sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante FUNPAZ IPS CLINICA DE SALUD MENTAL

12.10 DEBERES DEL RESPONSABLE Y/O ENCARGADO DEL TRATAMIENTO

Los deberes del Responsable y/o Encargado del Tratamiento, al momento de solicitar la autorización al Titular, son los siguientes:

- Informar al Titular en forma expresa y clara el Tratamiento al cual serán sometidos los datos personales y la finalidad del mismo; el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; los derechos que le asisten como Titular y la identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.
- Conservar la prueba de la autorización del Titular y de la información que le suministró al momento de obtener dicha autorización, así como la información bajo condiciones de seguridad para impedir adulteración, pérdida, consulta, uso o acceso fraudulento o no autorizado.
- Actualizar la información e informar de ello al Encargado del Tratamiento.
- Rectificar la información y comunicar lo pertinente al Encargado del Tratamiento.
- Suministrar al Encargado del Tratamiento la información autorizada.
- Tramitar las consultas y reclamos del Titular sobre el tratamiento de datos personales.

- Adoptar un manual interno de políticas y procedimientos para garantizar el cumplimiento de las normas de datos personales.

- Informar al Titular sobre el uso dado a sus datos.

- Poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización.
- Responder los requerimientos de la SIC mediante una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de la información; una descripción de las finalidades para las cuales es

recolectada la información y una explicación sobre la necesidad de recolectar los datos.

Designar el área encargada de asumir la función de protección de datos personales.

12.11 FINALIDADES DEL TRATAMIENTO

En nuestra calidad de responsables del Tratamiento desarrollamos políticas para efectuar el Tratamiento de los datos personales; hacemos constar las políticas de Tratamiento de la información en medio físico o electrónico, en un lenguaje claro y sencillo que ponemos en conocimiento de los Titulares.

Cualquier cambio sustancial en las políticas de Tratamiento será previa y oportunamente comunicado a los Titulares de los datos personales de una manera eficiente.

Por tanto, FUNPAZ IPS CLINICA DE SALUD MENTAL tendrá las siguientes finalidades en el Tratamiento de los datos personales:

- Realizar, a través de cualquier medio en forma directa, actividades de mercadeo, promoción y/o publicidad propia, venta, facturación, gestión de cobranza, recaudo, verificaciones y consultas, así como cualquier otra relacionada con nuestros servicios, actuales y futuros, para el cumplimiento de las obligaciones contractuales y de nuestro objeto social.

- Generar una comunicación óptima en relación con nuestros servicios y demás actividades.

- Evaluar la calidad de nuestro servicio, satisfacción y otras relacionadas con nuestros servicios.

- Prestar asistencia y servicio personalizado a nuestros clientes.

- Realizar las gestiones necesarias para dar cumplimiento a las obligaciones inherentes a los servicios contratados con FUNPAZ IPS CLINICA DE SALUD MENTAL.

- Cumplir con las obligaciones contraídas con nuestros clientes, proveedores, aliados, sus filiales y demás terceros públicos y/o privados, relacionados directa o indirectamente con el objeto social de FUNPAZ IPS CLINICA DE SALUD MENTAL.

- Informar sobre cambios de servicios relacionados con el giro ordinario de los negocios de FUNPAZ IPS CLINICA DE SALUD MENTAL.

- Facilitar la correcta ejecución de las prestaciones de los servicios y productos contratados.

El tipo de tratamiento que se realiza a los datos personales contempla lo siguiente, Compartir la información con:

- El o los encargados del tratamiento.

- Las personas jurídicas que tengan la calidad de proveedores, aliados, y terceros relacionados directa o indirectamente con el objeto social de FUNPAZ IPS CLINICA DE SALUD MENTAL.

- Las filiales y subsidiarias de FUNPAZ IPS CLINICA DE SALUD MENTAL

- Las personas con las que FUNPAZ IPS CLINICA DE SALUD MENTAL adelante gestiones para efectos de dar cumplimiento a sus obligaciones comerciales, contractuales, legales, administrativas y demás.

- Los terceros que manejan bases de datos para las finalidades establecidas en el presente Manual.

- Cumplir con las disposiciones normativas sobre transferencia de datos a terceros países en caso que dicha transferencia sea necesaria.

- Proveer información a las autoridades que lo soliciten expresamente y en ejercicio de sus funciones o para responder requerimientos administrativos y/o judiciales.

12.12 IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

FUNPAZ IPS CLINICA DE SALUD MENTAL, ha desarrollado aplicaciones y procedimientos internos para ofrecer medidas de seguridad en la protección y tratamiento de los datos personales consignados en las bases de datos y mitigar el riesgo de acceso y/o uso indebido, fraudulento o no autorizado sobre los datos personales.

12.13 MODIFICACIONES DEL MANUAL

FUNPAZ IPS CLINICA DE SALUD MENTAL, se reserva el derecho de modificar en cualquier momento y de forma unilateral, el presente Manual o cualquier política o procedimiento relativo al Tratamiento de datos personales, evento que comunicará oportuna y debidamente a los Titulares antes de su aplicación.

12.14 FECHA DE VIGENCIA

El presente Manual de Políticas y Procedimiento sobre el Tratamiento de Datos Personales rige a partir del momento en que mediante Acto Administrativo sea aprobado por la Gerencia y su junta directiva, como documento técnico de seguridad informática, el cual deberá ser revisado y actualizado conforme a las exigencias y necesidades de la clínica de salud mental FunPaz IPS.

12.15 LEGISLACION ADICIONAL APLICABLE (LEYES, ARTICULOS, DECRETOS)

Constitución Política, artículo 15.
Ley 1266 de 2008
Ley 1581 de 2012
Decretos Reglamentarios 1727 de 2009 y 2952 de 2010,
Decreto Reglamentario parcial 1377 de 2013
Sentencias C – 1011 de 2008, y C - 748 del 2011, de la Corte Constitucional
la **Sentencia T-161 / 1993, reiterada en la Sentencia T-1051 /2008**,
LEY 1616 DE 2013
Resolución 1995 de 1999

LEY 1616 DE 2013

TÍTULO II. <sic, es I>
DERECHOS DE LAS PERSONAS EN EL ÁMBITO DE LA SALUD MENTAL.

ARTÍCULO 6o. DERECHOS DE LAS PERSONAS. Además de los Derechos consignados en la Declaración de Lisboa de la Asociación Médica Mundial, la Convención sobre los Derechos de las Personas con Discapacidad y otros instrumentos internacionales, Constitución Política, y la Ley General de Seguridad Social en Salud son derechos de las personas en el ámbito de la Salud Mental:

15. Derecho a la confidencialidad de la información relacionada con su proceso de atención y respetar la intimidad de otros pacientes.

LEY 23 DE 1981

El artículo 34 de la Ley 23 de 1981 definió la historia clínica en los siguientes términos:

"ARTICULO 34*. La historia clínica es el registro obligatorio de las condiciones de salud del paciente.* ***Es un documento privado sometido a reserva*** *que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley".*

Resolución 1995 de 1999

Del mismo modo, el artículo 1° de la Resolución 1995 de 1999, señala:

"ARTÍCULO 1.- DEFINICIONES. *La Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.*

(…)"

En armonía con las disposiciones que vengo de transcribir, el artículo 14 de la mencionada Resolución, dispuso:

"ARTÍCULO 14.- ACCESO A LA HISTORIA CLÍNICA*. Podrán acceder a la información contenida en la historia clínica, en los términos previstos en la Ley:*

1) El usuario.

2) El Equipo de Salud.

3) Las autoridades judiciales y de Salud en los casos previstos en la Ley.
4) Las demás personas determinadas en la ley.

PARAGRAFO. *El acceso a la historia clínica, se entiende en todos los casos, única y exclusivamente para los fines que de acuerdo con la ley resulten procedentes, debiendo en todo caso, mantenerse la reserva legal."*

Como puede advertirse, entre las personas que relaciona el art. 14 de la mencionada Resolución con posibilidades de acceder la historia clínica, no está incluido el empleador ni el personal administrativo de la EPS ni las IPS que tramitan las incapacidades de los afiliados.

En la **Sentencia T-161 / 1993, reiterada en la Sentencia T-1051 /2008**, la Corte Constitucional dijo: *"La historia clínica, su contenido y los informes que de la misma se deriven, están sujetos a reserva y, por lo tanto, sólo pueden ser conocidos por el médico y su paciente. (…)."*

Y en la sentencia T-114/093, en uno de sus apartes, señaló:
"(…) Con todo, ha de tomarse en consideración que la historia clínica que reposa en la entidad demandada constituye, en principio, no sólo un documento privado sometido a reserva, que únicamente puede ser conocido por el paciente y la institución, y excepcionalmente por un tercero, con autorización de dicho paciente u orden de autoridad competente, sino que constituye el único archivo o fuente de información donde lícitamente reposan todas las evaluaciones pruebas, diagnósticos e intervenciones realizadas al paciente, al igual que los procedimientos y medicamentos que le fueron suministrados. (…)"

De igual manera, en la Sentencia T-158 A de 2008, la misma Corporación afirmó:
"El carácter reservado de la historia clínica, entonces, se funda en la necesidad de proteger el derecho a la intimidad del individuo sobre una información que, en

principio, únicamente le concierne a él y que, por tanto, debe ser excluida del ámbito de conocimiento público. (…)"

De conformidad con lo anterior, aunque en principio el paciente y su médico son los únicos que pueden conocer el contenido de la historia clínica, la ley ha previsto que excepcionalmente pueden tener acceso a la misma las personas a quienes el paciente autorice, y aquellas a las que la propia ley ha autorizado, como es el caso del equipo de salud y las autoridades judiciales. La prohibición de que personas distintas de las mencionadas puedan conocer la información contenida en la historia clínica, obedece a la necesidad de proteger el derecho a la intimidad de su titular, pues contiene información de carácter confidencial.

Ahora bien, sobre la situación que se ha venido presentando de que para el reconocimiento de las incapacidades algunas EPS le exigen al empleador que adjunte a éstas copia de la historia clínica del trabajador incapacitado, lo cual conduce a que el patrono repita contra el trabajador esta exigencia, dio lugar a que el Ministerio de Salud y Protección Social hiciera la siguiente precisión:

"En este orden de ideas, debe precisarse que ninguna Entidad Promotora de Salud – EPS podrá exigirle al empleador copia de la historia clínica de sus trabajadores, con el fin de reconocer la prestación económica derivada de la incapacidad, licencia de maternidad y paternidad, razón por la que a su vez, el empleador tampoco podrá hacer dicha exigencia al trabajador, en el entendido, que adjuntar la copia de la historia clínica no es un requisito para el reconocimiento de dichas prestaciones económicas.

(Fuente: Concepto 201411601165391 – 15 de agosto de 2014 – – Ministerio de Salud y Protección Social)

Ley 23 De 1981- Art. 34, Por lo cual se dictan Normas en Materia de Ética Médica, donde La historia clínica es el registro obligatorio de las condiciones de salud del paciente. Es un documento privado, sometido a reserva, que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley en 1981.

Ley100 de 1993, Por la cual la Seguridad Social Integral es el conjunto de instituciones, normas y procedimientos, de que disponen la persona y la comunidad para gozar de una calidad de vida, mediante el cumplimiento progresivo de los planes y programas que el Estado y la sociedad desarrollen para proporcionar la cobertura integral de las contingencias, especialmente las que menoscaban la salud y la capacidad económica, de los habitantes del territorio nacional, con el fin de lograr el bienestar individual y la integración de la comunidad en 1993.

Resolución 1995 de 1998- Art. 14, Por la cual se establecen normas para el manejo de la Historia Clínica. Requisitos para el acceso a la historia clínica en 1999.

Resolución 1715 de 2005 -Art. 2, Retención y tiempo de conservación. La historia clínica debe conservarse por un periodo mínimo de diez (10) años, contados a partir de la fecha de la última atención. Mínimo tres (3) años en e l archivo de gestión del prestador de servicios de salud, y mínimo siete (7) años en el archivo central en 2005.

Finalidad de la historia clínica

La historia clínica tiene como finalidad primordial recoger datos del estado de salud del paciente con el objeto de facilitar la asistencia sanitaria. El motivo que conduce al médico a iniciar la elaboración de la historia clínica y a continuarla a lo largo del tiempo, es el requerimiento de una prestación de servicios sanitarios por parte del paciente.

Puede considerarse que la historia clínica es el instrumento básico del buen ejercicio sanitario, porque sin ella es imposible que el médico pueda tener con el paso del tiempo una visión completa y global del paciente para prestar asistencia.

No obstante, aunque el objetivo primordial de dicho documento es el asistencial, no pueden ni deben obviarse otros aspectos asistenciales de la historia clínica:

a.- Docencia e investigación: a partir de las historias clínicas pueden realizarse estudios e investigaciones sobre determinadas patologías, publicaciones científicas.

b.- Evaluación de la calidad asistencial: la historia clínica es considerada por las normas deontológicas y por las normas legales como un derecho del paciente derivado del derecho a una asistencia médica de calidad. Puesto que de trata de un fiel reflejo de la relación médico-paciente así como un registro de la actuación médico-sanitaria prestada al paciente, su estudio y valoración permite establecer el nivel de calidad asistencial prestada.

c.- Administrativa: la historia clínica es elemento fundamental para el control y gestión de los servicios médicos de las instituciones sanitarias.

d.- Médico-legal:
Se trata de un documento público/semipúblico: estando el derecho al acceso limitado

Puede considerarse como un acta de cuidados asistenciales
· Existe obligación legal de efectuarla por normativas vigentes: Ley General de Sanidad, Ordenación de prestaciones sanitarias, Derechos de los Usuarios, Código De ontológico Médico, Normas Internacionales.

Elemento de prueba en los casos de responsabilidad médica profesional: tiene un extraordinario valor jurídico en los casos de responsabilidad médica profesional, al convertirse por orden judicial en la prueba material principal de todos los procesos de responsabilidad profesional médica, constituyendo un documento médico legal fundamental y de primer orden. En tales circunstancias la historia clínica, es el elemento que permite la evaluación de la calidad asistencial tanto para la valoración de la conducta del médico como para verificar si cumplió con el deber de informar, de realizar la historia clínica de forma adecuada y eficaz para su finalidad asistencial, puesto que el incumplimiento de tales deberes también constituye causa de responsabilidad profesional.

Testimonio documental de ratificación/veracidad de declaraciones sobre actos clínicos y conducta profesional.

Instrumento de dictamen pericial: elemento clave en la elaboración de informes médico legales sobre responsabilidad médica profesional. El objeto de estudio de todo informe pericial sobre responsabilidad médica profesional es la historia clínica, a través de la cual se valoran los siguientes aspectos: enumeración de todos los documentos que la integran, reconstrucción de la historia clínica, análisis individualizado de los actos médicos realizados en el paciente, personas que intervinieron durante el proceso asistencial, etc.

El incumplimiento o la no realización de la historia clínica, puede tener las siguientes repercusiones:

Clínico-asistencial, por incumplimiento de la normativa legal
Defecto de gestión de los servicios clínicos
Riesgo de potencial responsabilidad por perjuicios al paciente, a la institución, a la administración

Riesgo médico legal objetivo, por carencia del elemento de prueba fundamental en reclamaciones médicas.

RESOLUCIÓN 3047 DE 2008 NUMERALES 4 y 15 DEL ANEXO TÉCNICO NO. 5 SOPORTES DE LAS FACTURAS

4. Resumen de atención o epicrisis: Resumen de la historia clínica del paciente que ha recibido servicios de urgencia, hospitalización y/o cirugía y que debe cumplir con los requerimientos establecidos en las Resoluciones 1995 de 1999 y 3374 de 2000, o las normas que las sustituyan, modifiquen o adicionen.

15. Historia clínica: es un documento privado, obligatorio y sometido a reserva en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Solo podrá ser solicitada en forma excepcional para los casos de alto costo.

Ley 594 de 2000 (Ley de archivos)

LEY 594 DE 2000
(julio 14)
Diario Oficial No. 44.093, de 20 de julio de 2000
Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

TITULO I.

OBJETO, AMBITO DE APLICACION, DEFINICIONES FUNDAMENTALES Y PRINCIPIOS GENERALES

ARTICULO 1o. OBJETO. La presente ley tiene por objeto establecer las reglas Y principios generales que regulan la función archivística del Estado.

ARTICULO 2o. AMBITO DE APLICACIÓN. La presente ley comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley.

Ley 527 de 1999 (Comercio Electrónico del 18 Agosto)

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

ARTÍCULO 6º. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

ARTÍCULO 8º. Original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos.

Artículo 257 del código penal (Acceso ilegal a las telecomunicaciones)

Código Penal

Artículo 257. De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones

El que, sin la correspondiente autorización de la autoridad competente, preste, acceda o use servicio de telefonía móvil, con ánimo de lucro, mediante copia o reproducción de señales de identificación de equipos terminales de estos servicios, o sus derivaciones, incurrirá en prisión de cuatro (4) a diez (10) años y en multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes.

En las mismas penas incurrirá el que, sin la correspondiente autorización, preste, comercialice, acceda o use el servicio de telefonía pública básica local, local extendida, o de larga distancia, con ánimo de lucro.

Iguales penas se impondrán a quien, sin la correspondiente autorización, acceda, preste, comercialice, acceda o use red, o cualquiera de los servicios de telecomunicaciones definidos en las normas vigentes.

PARÁGRAFO 1o. No incurrirán en las conductas tipificadas en el presente artículo quienes en virtud de un contrato con un operador autorizado comercialicen servicios de telecomunicaciones.

PARÁGRAFO 2o. Las conductas señaladas en el presente artículo, serán investigables de oficio.

13. POLITICAS DE SEGURIDAD DE BACKUP

El Backup de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre.

Como siempre, será necesario realizar un análisis Costo/Beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backup, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos

Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.

1. Actualmente en la Clínica de salud mental FunPaz IPS, se cuenta con la siguiente hoja de ruta para elaborar los backups de forma continua, es de aclarar, que con el nuevo proyecto de infraestructura y de ordenamiento lógico perimetral del nuevo servidor, esta ruta o guía de backup cambiará:

A continuación presentamos la ruta para generar el backup, la localización, la forma y el contenido del mismo.

Se ingresa al equipo, nos dirigimos a la unidad E, para que posteriormente aparezca la unidad de datos quien almacena las carpetas con los archivos.

Copiamos los datos para pegarlos en la unidad del disco externo.

Enseguida se abre la unidad del disco duro, nos vamos para CS ,buscamos la carpeta con el mes correspondiente y pegamos.

Es de resaltar que la persona idónea para realizar dicho backup es del área de sistemas, esta a su vez, es quien responderá por la información y su correspondiente respaldo.

2. Se debe reposar la copia de seguridad en las instalaciones de FunPaz de tres formas diferentes, la primera en una partición diferente a la principal en el disco duro del pc (regularmente disco local D), la segunda es un backup automático realizado por el programa Syncbackup el cual realiza un copiado de los documentos del funcionario a un computador dedicado solo a guardar la información de estos archivos, y a tercera es una copia en un disco externo.

3. Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.

4. El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.

5. Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.

6. Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.

7. Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se debe encriptar antes de respaldarse.

8. Se debe de contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.

9. Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:

8.1 Modalidad Externa: otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.

8.2 Modalidad Interna: se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

14. POLITICA DEL USO DE INTERNET

El Internet es una herramienta cuyo uso autoriza la institución FunPaz IPS en forma extraordinaria, puesto que contiene ciertos peligros, Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas.

14.1 RESPONSABILIDADES DEL ÁREA DE SISTEMAS:

a) Se asegurará de coordinar con los encargados de áreas, las páginas de Internet a las que puede tener acceso el personal bajo su cargo, bloqueando aquellas páginas que no sean relevantes para el desempeño de las funciones.
La finalidad de poder darle mejor uso a este tipo de herramientas es el poder optimizar el tiempo y los recursos dentro de la institución, de igual forma, se podrá evitar mediante estas descargas, virus e intrusos que quieran afectar la información de la Clínica.

b) Deberá monitorear el acceso de las páginas de internet por parte del personal e informar cualquier violación de acceso, vía correo electrónico a los encargados de las áreas.

c) Deberá informar vía correo electrónico o personalmente al encargado de área de sistemas, en caso de incurrir en una falta se le informará de manera escrita al jefe directo de cada área o a quien corresponda. Los casos continuos de violación de acceso a internet a páginas no relacionadas con el trabajo institucional como, por ejemplo: de juegos, de música, descargas, videos, entre otras; con la finalidad de que se tomen las medidas de lugar, es importante aclarar, que el empleado tendrá la seguridad de que se le estará respetando sus derechos y su privacidad de la información, y se le notificara en prima instancia algún procedimiento indebido.

d) Dará seguimiento a la plataforma de internet, notificando a las áreas los inconvenientes presentados en la misma.

Se debe aplicar una política que procure la seguridad y realizar monitoreo constante, por lo que se debe tener en cuenta lo siguiente:

A continuación se describen las políticas que se deben tener en cuenta para el uso adecuado de este Importante servicio por parte de los usuarios:

14.2 RESPONSABILIDADES DE LOS USUARIOS:

- El acceso a internet en horas laborales según como corresponda el turno si es personal asistencial o si corresponde al empleado administrativo) es de uso solo laboral no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.

- No acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista etc. o que estén fuera del contexto laboral.

- En ningún caso recibir ni compartir información en archivos adjuntos de dudosa procedencia, esto para evitar el ingreso de virus al equipo.

- No descargar programas, demos, tutoriales, que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado.

- La descarga de ficheros, programas o documentos que contravengan las normas de la Hospital sobre instalación de software y propiedad intelectual.

- Ningún usuario está autorizado para instalar software en su ordenador. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo a la Oficina de Sistemas que se encargará de realizar las operaciones oportunas.

- Los empleados de la clínica FunPaz tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.

- Los usuarios de la Clínica FunPaz, que requieran de una autorización especial, ya que, por cuestiones laborales requiera ciertos programas, deberá llenar el formato de autorización de páginas en internet ya sea por vía correo electrónico o personalmente.

- Los casos que se presenten y que estén vinculados al trabajo y no estén contemplados en este Manual de Políticas, serán atendidos o resueltos por la Dirección Ejecutiva de la Institución.

- Ningún empleado debe instalar ningún programa para ver vídeos o emisoras de televisión vía Internet y de música. (YouTube, Ares, REAL AUDIO, BWV, Netflix, Spofity, etc.).

- No debe usarse el Internet para realizar llamadas internacionales (Dialpad, skype, NET2PHONE, FREEPHONE, etc.), excepto que se requiera la llamada para uso exclusivo laboral y a beneficio de la institución.

15. POLITICAS DE USO DE COMPUTADORES, IMPRESORAS Y PERIFÉRICOS

- La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general; no DEBE ser utilizado en funciones diferentes a las institucionales.

- Los usuarios no DEBEN instalar, suprimir o modificar el software originalmente No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. A no ser que sean periféricos como memorias, discos duros externos o teras que se requieran para beneficio de la institución.

- Es competencia de la Oficina de sistemas, el retiro o cambio de partes.

- No se puede utilizar Memorias y/o discos extraíbles traídos de sitios externos a la clínica, sin la previa revisión por parte del administrador del sistema para control de circulación de virus.

- No es permitido destapar o retirar la tapa de los equipos, por personal diferente a la Oficina de sistemas o bien sus asistentes o sin la autorización de esta,

- Los dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, sin antes informar de la Oficina de sistemas.

- Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.

- Es estrictamente obligatorio, informar oportunamente a la Oficina de sistemas la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad de los procesos.

- El reporte de las novedades debe realizarse a la Gerencia de Informática tan pronto se presente el problema.

- Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.

- Los protectores de pantalla y tapiz de escritorio, serán establecidos por la oficina de sistemas y deben ser homogéneos para todos los usuarios.

- Ningún funcionario podrá formatear los discos duros de los computadores.

- Ningún funcionario podrá retirar o implementar partes sin la autorización de la Oficina de Sistemas.

16. CUSTODIA Y TENENCIA DE ACTIVOS INFORMÁTICOS

Es responsabilidad del área de sistemas de la entidad, salvaguardar y garantizar el buen uso de los equipos y demás activos de la empresa.

El uso indebido de los recursos informáticos puede afectar negativamente el funcionamiento de los equipos de oficina (PC), la red, los servidores por tanto:

a) Custodiará todos los activos informáticos de la Clínica de salud mental FunPaz

b) Asignará los equipos informáticos a todos los usuarios, de acuerdo con los requerimientos de las áreas.

c) Verificará que no le sea asignado un mismo activo informático a más de un Usuario, para ello la entidad cuenta con unos formatos que el usuario debe diligenciar, firmar y aceptar el contrato.

d) Verificará que los Usuarios sean empleados regulares de la Clínica de salud mental FunPaz, así como contratistas externos, consultores, etc.

e) Llevará el control de los equipos informáticos portátiles (Laptop) asignados al personal gerencial que realice trabajos fuera de la Institución, para ello la entidad cuenta con unos formatos que el usuario debe diligenciar, firmar y aceptar el contrato.

f) Notificará, vía electrónica o cualquier otra vía los inconvenientes o anomalías presentadas con los equipos, accesorios, impresoras, sistemas, entre otros.

17. TRASLADO DE ACTIVOS INFORMÁTICOS FUERA DE LA CLINICA DE SALUD MENTAL FUNPAZ.

Al momento de recibir una solicitud de las áreas, para el traslado de un equipo informático fuera de la institución, el compromiso de del área de sistemas de FunPaz, es el siguiente:

17.1 RESPONSABILIDAD DEL AREA DE SISTEMAS:

a) Verificar el estado de los equipos tecnológicos a ser entregados a las áreas, a través del Formato Movimientos de Activos (Equipos), para comprobar su salida y recepción en buen estado.

17.2 RESPONSABILIDAD DE LOS USUARIOS:

El compromiso de los usuarios al momento de solicitar el traslado de un equipo informático fuera de la institución son los siguientes:

a) Deberá llenar completamente hasta la casilla “Descripción del Equipo” en el Formato Movimientos de Activos (Equipos) el cual debe ser aprobado por el Área de sistemas.

b) Deberá reportar cualquier daño o/y deterioro de los equipos informáticos facilitados.

18. POLITICA POR ROBO O PÉRDIDA DE EQUIPO

a) A partir de las políticas definidas, el área de sistemas de FunPaz, determinará los pasos a seguir para el inventario de los equipos que se reporten como sustraídos. (Se le suministrara al empleado un formato de descarga de los hechos ocurridos y el procedimiento a seguir)

b) El usuario de un equipo asignado deberá reportar dentro de veinticuatro (24) horas cualquier pérdida o sustracción del mismo, tanto al área Administrativa como a la División de sistemas, y estos a la gerencia.

c) El área de sistemas y de talento humano se encargará de realizar los procesos pertinentes para que se establezca responsabilidad ante dicha pérdida.

d) Ante el caso de que se determine responsabilidad por parte del usuario de dicha perdida, se empoderara a la Dirección Ejecutiva como a la Sección de Recursos Humanos de la institución para que se proceda con la aplicación de Las medidas que se consideren correspondientes.

19. SOPORTE TÉCNICO A LOS EQUIPOS ASIGNADOS

Las responsabilidades descritas constituyen la normativa ante las solicitudes recibidas para la asistencia de soporte técnico a los equipos asignados a los usuarios.

19.1 RESPONSABILIDAD DEL AREA DE SISTEMAS:

Será responsabilidad del área de sistemas de FunPaz por:

a) Todas las solicitudes de Soporte Técnico, deberán ser remitidas, vía correo Electrónico o llenando el formato de soporte, quien le dará las instrucciones necesarias al personal técnico bajo su cargo (si es necesario y existe personal)

b) Deberá dar un tiempo de respuesta a cada una de las solicitudes que hayan sido notificadas por los usuarios en un plazo no mayor de un (1) día laborable.

c) Cuando el área de sistemas considere que el reporte de avería es mínimo, se podrá proceder con la reparación de inmediato.

d) Deberá de asegurar que el usuario este satisfecho con el servicio prestado

e) Deberá recibir e instalar los equipos tecnológicos solicitados por las diferentes áreas de la Institución.

f) Se encargará de revisar todos los equipos, accesorios, programas, entre Otros.

19.2 RESPONSABILIDAD DE LOS USUARIOS

La responsabilidad de los usuarios ante la solicitud de asistencia del área de sistemas es la siguiente:

a) Solicitará, de manera formal vía correo electrónico o mediante oficio al área de sistemas, las solicitudes de modificaciones servicio técnico, así como cualquier anormalidad en su equipo, con copia a su superior inmediato.

b) Solicitará todos los servicios de soporte tecnológicos, a través de correo electrónico. En caso que el equipo no responda.

20. BIBLIOGRAFIA

HUERTAS LEONARDO. Políticas de seguridad [en línea].
http://www.slideshare.net/SamuraiBlanco/politicas-seguridad-leonardo-huertas

LEY 734 de 2002 Código Único Disciplinario

LEY 1273 de 2009.Delitos Informáticos