MEDINUCLEAR®

Imágenes Diagnósticas

"Mejores imágenes. Mejores resultados"

PROCEDIMIENTO SEGURIDAD Y TRAZABILIDAD DE LA INFORMACIÓN
PRSI002

ELABORÓ	REVISÓ	APROBÓ
ALVARO TORRES ASISTENTE INFORMÁTICO	**MARIA ALEJANDRA PORTILLA** COORDINADORA DE CALIDAD **YAMILE REVELO** COORDINADORA ADIMINITRATIVA JURIDICA	**JAVIER PAZ** GERENTE

VIGENCIA	VERSIÓN	CONTROL DE CAMBIO
7/12/2020	**2**	Se modifica objetivo, alcance, responsables, se adicionan definiciones y se actualiza Procedimiento en cumplimiento de la Ley de Protección de Datos, reemplazando la vigencia 15/12/2018 - versión 1

1. OBJETIVO

El presente documento desarrolla el precepto constitucional de “habeas data” y protege todo lo relacionado con el conocimiento, actualización, rectificación y oposición de la información personal contenida en bases de datos y archivos, el cual ha sido desarrollado y protegido mediante la Ley Estatutaria 1581 de 2012, (en adelante la “LEPDP”). El derecho de *habeas data* debe entenderse como un derecho fundamental autónomo que se compone de dos elementos: la autodeterminación informática y la libertad.

Por lo tanto, este manual tiene como objeto garantizar el adecuado cumplimiento de la LEPDP, el ejercicio de los derechos de los titulares de información personal y, a su vez, la protección de la información y de los sistemas de información que se consideren críticos e importantes dentro de la organización del acceso, utilización, divulgación y/o destrucción no autorizada.

2. ALCANCE

Aplica para todo el personal de MEDINUCLEAR que maneje información en mediomagnético y físico y a todos los datos de carácter personal registrados en soportes, físicos o digitales, que sean susceptibles de ser tratados por MEDINUCLEAR como responsable de dichos datos. El contenido del presente documento no se aplicará a las bases de datos o archivos indicados en el artículo 2 de la Ley 1581 de 2012.

3. RESPONSABLES

- Profesional administrativo de sistemas
- Líderes de ProcesosCoordinadores
- Personal con acceso a la información en medio magnético.

4. DEFINICIONES

AUTORIZACIÓN: Consentimiento previo, expreso e informado del titular de la información para llevar a cabo el tratamiento de los datos personales.

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de tratamiento. Este conjunto de datos se compone principalmente de documentos y textos impresos en papel o en formato digital.

CONSENTIMIENTO DEL TITULAR: Es una manifestación de la voluntad, informada, libre e inequívoca, a través de la cual el titular de los datos de carácter personal acepta que un tercero utilice su información.

CONSULTAS: Los titulares o sus causahabientes podrán consultar la información personal del titular que repose en cualquier base de datos.

COPIA DE SEGURIDAD: Es la actividad relacionada con realizar un duplicado de la información de forma segura, con el fin de salvaguardar la información ante cualquier eventualidad.

DATO PERSONAL: Se refiere a cualquier información asociada a una persona natural, identificada o identificable, relativa tanto a su identidad: nombre y apellidos, domicilio, filiación, entre otras, como a su existencia y sus ocupaciones: estudios, trabajo, enfermedades, entre otras.

DATO PÚBLICO: Es el dato calificado como tal por la Constitución o la ley y todos aquellos que no sean semiprivados o privados, de conformidad con la ley colombiana. Son públicos, entre otros, los datos contenidos en documentos públicos, gacetas y boletines judiciales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva y los relativos al estado civil de las personas.

DATO SEMIPRIVADO: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

DATO PRIVADO: Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular.

DATOS SENSIBLES: Para los propósitos de la presente política, se entiende por dato sensible todo aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, 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 promuevan 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.

DISCO DURO EXTERNO: Sistema de almacenamiento que permite almacenar datos de forma local la cual tiene como finalidad servir de respaldo.

ENCARGADO DEL TRATAMIENTO: Es quien gestiona los datos de carácter personal, pero no decide cómo, ni con qué fin. Su trabajo es operativo y se hace con base en las indicaciones e instrucciones del responsable del tratamiento.

FINALIDAD LEGÍTIMA: Serán las finalidades para las que el responsable tratará los datos personales, así como la base jurídica que legitima el tratamiento de los datos personales suministrados por el titular.

GOOGLE DRIVE: Servicio de almacenamiento y envío de archivos remoto con el cual se realizan las copias de seguridad de forma automática y sincronizada.

HABEAS DATA: Es el derecho que tiene todo titular de información de conocer, actualizar, rectificar u oponerse a la información concerniente a sus datos personales.

INFORMACIÓN CRÍTICA E IMPORTANTE: Es el activo más valioso que tiene la organización, el cual, si llegará a perderse o modificar indebidamente, afectaría a la misma de manera operativa, legal y financieramente.

PACS (*Picture Archiving and Communication System*): Un servidor PACS es un sistema de almacenamiento digital, transmisión y descarga de imágenes radiológicas.

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: Es un derecho fundamental que tienen todas las personas naturales. Busca la protección de su intimidad y privacidad frente a una posible vulneración por el tratamiento indebido de datos personales capturados por un tercero.

RECLAMO: El titular o sus causahabientes que consideren que la información contenida en una 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 o en el presente documento, podrán presentar un reclamo ante el responsable o el encargado 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 o el tratamiento de los datos personales.

TRATAMIENTO: Cualquier operación o procedimientos físicos o automatizados que permita captar, registrar, reproducir, conservar, organizar, modificar, transmitir los datos de carácter personal.

TITULAR DE LOS DATOS PERSONALES: Es la persona natural cuyos datos personales son objeto de tratamiento por parte de un tercero.

5. PRODUCTO

Información y sistemas informáticos con respaldo (copias de seguridad), en diferentes servidores

6. CLIENTES

Usuarios de los diferentes equipos de cómputo del Grupo Medinuclear, en donde se almacene información.

7. DOCUMENTOS RELACIONADOS

FORMATOS	
ODSI002	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES
FRSI002	FORMATO DE REGISTRO DE COPIAS DE SEGURIDAD
	FORMATO “AUTORIZACIÓN PARA SOLICITAR Y ACCEDER A LA HISTORIA CLÍNICA”

8. DERECHOS DE LOS TITULARES DE INFORMACIÓN PERSONAL.

Para garantizar la protección de los datos personales por parte de MEDINUCLEAR, los(as) titulares de la información personal tendrán los siguientes derechos:

- Conocer y acceder a sus datos personales que hayan sido objeto de un tratamiento.
- Actualizar sus datos personales que hayan sido objeto de un tratamiento.
- Rectificar los datos personales que hayan sido objeto de un tratamiento.
- Revocar la autorización y solicitar la supresión de sus datos personales, cuando en el tratamiento de estos no se hayan respetado los principios establecidos en la Ley 1581 de 2012.
- Solicitar prueba de la autorización otorgada para el tratamiento de sus datos personales.

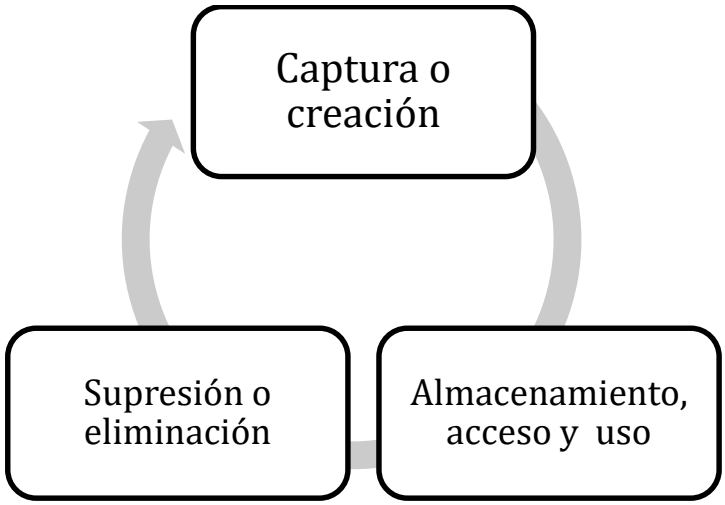
Estos derechos podrán ser ejercidos directamente por el titular de la información, su apoderado o su causahabiente de acuerdo con los procedimientos y canales establecidos por MEDINUCLEAR en la **Política de Protección de Datos Personales**, según el caso, siempre que se presente el documento idóneo para acreditar la calidad de titular o su representación, como lo es un poder o autorización firmado y autenticado ante notaria. Los titulares de la información o sus representantes podrán consultar, reclamar, modificar, actualizar, rectificar, suprimir o revocar la autorización otorgada respecto del tratamiento de los datos personales a través de los siguientes canales de comunicación, para lo cual deberá incluir en el asunto de su comunicación el término “consulta o reclamo de habeas data”:

Domicilio	Correo electrónico	Teléfono
Carrera 34 No. 11 A-12, Pasto (N)	gerencia@grupomedinuclear.com	(2) 7382043

De acuerdo con la normatividad vigente, el titular, apoderado o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio (SIC) una vez haya agotado el trámite de consulta o reclamo ante MEDINUCLEAR, en calidad de responsable o encargado del tratamiento de la información. La persona interesada o afectada que desee ejercer cualquiera de los derechos citados en este documento, podrá hacerlo por comunicación escrita a MEDINUCLEAR, acompañando dicha solicitud de su firma y copia de la identificación personal o documento similar que acredite su calidad de titular o representante.

9. POLÍTICAS DE SEGURIDAD DE LOS DATOS.

Para aplicar de manera adecuada las presentes medidas de seguridad de los datos, se deberá tener en cuenta el siguiente ciclo de vida de los datos:



9.1. Fase 1. Captura o creación:

La información tratada por MEDINUCLEAR puede tener diferentes fuentes de captura:

1) El titular, quien de manera directa o a través de su representante legal (aplica a menores de edad) entrega información de tipo personal.
2) A través de los consentimientos informados de los pacientes o usuarios.
3) Fuentes públicas de información.
4) Servicios de mensajería instantánea.
5) A través de los formularios incluidos en el sitio web: http://medinuclear.com.co/
6) A través de los formularios de proveedores o contratistas.

9.2. Fase 2. Almacenamiento, acceso y uso:

Los datos son tratados con la intención de almacenar y ordenar la información para posteriores usos, éstos se determinan en función de cómo MEDINUCLEAR pretenda conservar y utilizar la información. El inventario de bases de datos y archivos que almacenan datos personales sobre los cuales MEDINUCLEAR tiene la calidad de responsable del Tratamiento son de conocimiento del Oficial de Protección de Datos u Oficial de Cumplimiento y de cada una de las áreas responsables.

El acceso a los datos se refiere a la posibilidad de consultarlos, modificarlos y eliminarlos; estos tratamientos tienen como fin facilitar los posteriores usos que se han previsto para la información, por ejemplo: visualizar, imprimir, registrar, agrupar, filtrar, transferir, transmitir, analizar, calcular, cancelar, destruir, actualizar, transformar, entre otros. Los usos de la información se encuentran

definidos de forma específica en la Política de Tratamiento de Datos Personales, la cual se puede consultar en cualquier momento en los canales de comunicación mencionados en el presente documento.

En MEDINUCLEAR está prohibida la comercialización de cualquier base de datos personales sin la autorización expresa y escrita de la Junta Directiva y sin la autorización escrita de los titulares de la información.

9.3. Fase 3. Supresión o eliminación de la información:

Los datos son tratados con la intención de suprimirlos o eliminarlos de las bases de datos y archivos sobre los cuales MEDINUCLEAR tenga la calidad de responsable del tratamiento. Siempre que se pretenda eliminar o suprimir la información, se deberán tener en cuenta las siguientes recomendaciones:

- Los documentos que vayan a ser eliminados o destruidos deben estar protegidos hasta el momento de su destrucción física.
- El lugar que almacena los documentos que se pretenden eliminar debe contar con medidas de seguridad eficaces frente a posibles intromisiones exteriores.
- Los documentos no deben permanecer al descubierto, en el exterior de los edificios, así como no deben amontonarse en lugares de paso, ni en espacios abiertos accesible a quién no debe conocer esos datos.
- Todo papel u otro soporte físico que contenga datos personales y que vaya a ser arrojado al recipiente de basura, deberá previamente ser destruido de forma que la información no sea reutilizada o legible.
- El papel que se pretenda reciclar no debe contener datos personales; de lo contrario, debe ser destruido, no reconstruirlo.
- Todo papel u otro soporte físico que contenga datos personales solo podrá ser almacenado y destruido por las personas que estén debidamente autorizadas para ello.

10. DESCRIPCIÓN DE LA OPERACIÓN DE ACTIVIDADES

10.1. Procedimiento general de manejo de la información

- Los métodos de recolección de la información varían de acuerdo con el área que la maneja, junto con un responsable a cargo de esta.
- El almacenamiento de la información se realiza a través de los servidores de sus respectivas áreas, la información se respalda de manera local, también a través de la nube y, por último, por un medio externo como lo es un disco duro portátil de respaldo.
- El uso de la información es confidencial y está protegida por los debidos procedimientos de seguridad y contraseñas; por lo cual, cada profesional a cargo maneja usuarios con los cuales se realiza seguimiento de los movimientos de la información y se vela por la confidencialidad de la información.
- La información solo puede ser utilizada por los profesionales que tengan sus respectivos permisos y autorizaciones. Los encargados de cada área son responsables del tratamiento de datos que se requiera.

10.2. Procedimiento general de manejo de la información de empleados

- La base de datos automatizada de los *empleados* está ubicada en el área de gestión humana, con usuario, clave de acceso y es con acceso únicamente por parte del personal autorizado. Esta base de datos bajo la responsabilidad del líder de gestión humana de MEDINUCLEAR y contiene el registro de la información sensible de los colaboradores activos e inactivos y su grupo familiar primario.
- La documentación física en archivo se encuentra bajo custodia del área de gestión humana, con acceso solo del personal autorizado para los fines descritos en el tratamiento de datos.
- Los contratos de trabajo incluyen una cláusula donde el colaborador autoriza el tratamiento de los datos por parte de la MEDINUCLEAR, de acuerdo con las finalidades de la Política de Tratamiento de Datos Personales; además, contiene una cláusula de confidencialidad respecto de la información y datos personales que conocerá en ejercicio del cargo.
- La información de niños, niñas y adolescentes, requerida para el proceso de gestión de seguridad social, se encuentra con autorización de la representación legal / colaborador. El tratamiento de los datos entregados a las entidades encargadas de administrar la seguridad social de los colaboradores será responsabilidad de cada entidad receptora, entre estas: EAPB, AFP, Caja de compensación familiar.
- La constancia de entrega de información solicitada dentro del proceso de tratamiento de datos quedará archivada dentro de una A-Z llamada Documentos Soporte Tratamiento de datos Personales.

10.3. Tratamiento de los datos personales proporcionados por los usuarios y familiares o acompañantes a través de las IPS

- Base de datos sistematizada en el software de SALUDIPS, el aplicativo DATOS CLINICOS y REPORTES se crea con el aplicativo ubicado en el área de atención al usuario, admisiones y asignación de citas médicas, con un usuario designado con su respectiva clave de acceso.
- Esta base de datos cuenta con el registro de la información sensible de los usuarios atendidos en la Institución y bajo la responsabilidad del líder del archivo de MEDINUCLEAR.
- La documentación física se encuentra en archivo, con acceso restringido, solo del personal autorizado para los fines descritos en el tratamiento de datos, especialmente por la custodia de la información de la historia clínica.
- Se cuenta con el formato “autorización para solicitar y acceder a la historia clínica” donde el usuario, de manera clara y expresa, autoriza a las personas que podrán tener acceso a la información confidencial consignada en su historia clínica.
- La información de niños, niñas y adolescentes, atendidos en MEDINUCLEAR deberá estar respaldada por el adulto que actúa como responsable del menor, aportando el respectivo documento que acredite dicha calidad.
- El tratamiento de los datos personales solicitados y autorizados por parte del titular para fines comerciales estará en una base de datos automatizada con clave de acceso y manejo de personal autorizado.

10.4. Tratamiento de los datos personales proporcionados por las entidades responsables de pago, accionistas y proveedores de MEDINUCLEAR

- La base de datos sistematizada en aplicativa contable del software SISCONFI (clientes y proveedores) y SIIFNET (Nómina) esta automatizada para los proveedores y accionistas y ubicada en el área administrativa y contable de la Institución, con usuario asignado y clave de acceso sólo del personal previamente autorizado.
- Esta base de datos cuenta con los registros de la información de los proveedores, clientes y accionistas y bajo la responsabilidad del área administrativa y contable de MEDINUCLEAR.
- La documentación física se encuentra bajo custodia del personal administrativo y contable con acceso solo del personal previamente autorizado para los fines descritos en la Política de tratamiento de datos.
- La constancia física de entrega de información solicitada dentro del proceso de tratamiento de datos quedará archivada dentro de una A-Z llamada Documentos Soporte Tratamiento de datos Personales.

10.5. Tratamiento de los datos de Líderes de proceso y Coordinadores

No.	Actividad	Responsable	Registro
1.	**IDENTIFICACIÓN DE INFORMACIÓN CRÍTICA E IMPORTANTE:** Determinar la información que maneje cada líder o coordinador y sea tomada de los sistemas de información propios de la empresa o documentos externos a cuál se le realizará una copia de seguridad local, en la nube y/o en disco duro externo y se procederá a diligenciar el formato de registro de copias de seguridad FRSI002, especificando en que días se guardó el archivo y/o carpeta donde se encuentre la misma.	Líderes deprocesos Coordinadores Administrativo de sistemas	FRSI002 formato de registro de copias de seguridad
2.	**VERIFICACIÓN DE COPIAS DE SEGURIDAD**: Verificar si se está realizando la copia de seguridad local en la nube y/o en disco duro externo, de acuerdo con lo estipulado por cada líder en el formato de registro de copias de seguridad FRSI002.	Administrativo de sistemas	FRSI002 formato de registro de copias de seguridad
3.	**RESTAURACIÓN DE COPIAS DE SEGURIDAD:** Proceder con la restauración de la información como sería la recuperación local, restauración de *back up* en la nube o restauración de *back up* en el	Administrativo de sistemas	

	disco duro externo de respaldo, si esta llegase a presentar alguna contingencia, perdida y/o daño, total o parcialmente, los líderes de cada proceso notificaran al administrativo de sistemas a través de los medios estipulados, inmediatamente después de conocidos los hechos, el Oficial de Protección de Datos realizará los respectivos reportes a la Superintendencia de Industria y Comercio.		

10.6. Tratamiento de los datos de Servicio farmacéutico

<table>
<tr><th>No.</th><th>Actividad</th><th>Responsable</th><th>Registro</th></tr>
<tr><td>1</td><td>NIVELES DE ACCESO:

La Carpeta “Servicio Farmacéutico”, donde se almacena toda la información de esa área, se encuentra alojada en el servidor de archivos que está custodiada por el Administrativo de sistemas.
La información almacenada en esta carpeta es suministrada por los sistemas internos de la empresa y almacenada en el servidor de información correspondiente.
El acceso y uso de la información de dicha carpeta está condicionado según el cargo y la información allí contenida de la siguiente manera:
<table>
<tr><td>CARPETA</td><td></td></tr>
<tr><td>Químicos</td><td>Químicos Farmacéuticos</td></tr>
<tr><td>Regentes</td><td>Regentes de Farmacia y Químicos Farmacéuticos</td></tr>
<tr><td>Auxiliares</td><td>Auxiliares de farmacia, Regentesde Farmacia y Químicos Farmacéuticos</td></tr>
</table></td><td>Administrativo de Sistemas</td><td></td></tr>
<tr><td>2.</td><td>CONFIDENCIALIDAD PLANTILLA EXCEL:

Conceder a las plantillas un formato predeterminado en el cual el personal autorizado del servicio farmacéutico solo diligenciara los campos previamente habilitados ya que actualmente todos los paquetes técnicos que se manejan en el servicio</td><td></td><td></td></tr>
</table>

	farmacéutico están digitalizados en formato Excel Todos los paquetes técnicos tienen una hoja oculta, la cual contiene las firmas y las contraseñas del personal del servicio, esta contraseña es individual y es asignada de forma personal y con aval del asistente técnico. En caso de que se requiera realizar algún cambio en la contraseña o en la plantilla en general se deberá informar al administrativo de sistemas. Al final del proceso los paquetes técnicos diligenciados deben convertirse a archivos tipo PDF, para evitar cambios en la información.	Administrativo de Sistemas	
3.	**COPIA DE SEGURIDAD EN DISCO DURO:** Determinar las fechas en que se realizarán las copias de seguridad de la carpeta "Servicio Farmacéutico" tanto con el almacenamiento en la nube como con en el disco duro externo y el mismo se hará responsable de la custodia de este. El administrativo de sistemas verificará que estas copias se estén realizando de forma correcta y la fecha estipulada para tal fin.	Químico Farmacéutico	FRSI002 FORMATO DE REGISTRO DE COPIAS DE SEGURIDAD
4.	**COPIA DE SEGURIDAD EN GOOGLE DRIVE:** Programar la sincronización de archivos en google drive para guardar los cambios que se efectúen de manera diaria en la carpeta de "Servicio Farmacéutico", la cual está enlazada con la Cuenta de correo del administrativo de sistemas.	Administrativo de Sistemas	
5.	**VERIFICACIÓN DE LA INFORMACIÓN:** Revisar las copias deseguridad en las plataformas de respaldo de información en la nube (Google drive) y en el almacenamiento externo (Disco Duro), de acuerdo con lo descrito en el formato FRSI002.	Administrativo de Sistemas	
6.	**RESTAURACIÓN DE LA INFORMACIÓN:** Informar inmediatamente por parte de los químicos farmacéuticos si por algún motivo la carpeta de "Servicio Farmacéutico" se llegase a dañar y/o sufra cualquier contingencia al administrativo de sistemas para que esté inicie el respectivo proceso de	Administrativo de Sistemas	

	restauración de la carpeta o del archivo solicitado. Inmediatamente después de conocidos los hechos, el Oficial de Protección de Datos realizará los respectivos reportes a la Superintendencia de Industria y Comercio.		

10.7. Tratamiento de los datos de Servidor PACS

No.	Actividad	Responsable	Registro
1.	Ingresar al servidor PACS está autorizado únicamente para el administrativo de sistemas. En este servidor se encuentran los aplicativos de administrador de usuario, administrador de imágenes y las carpetas donde se almacenan las imágenes diagnósticas.	Administrativo de Sistemas	FRSI002 FORMATO DE REGISTRO DE COPIAS DE SEGURIDAD
2.	**COPIA DE SEGURIDAD EN GOOGLE DRIVE:** Programar la sincronización de las carpetas en google drive para guardar las nuevas imágenes diagnósticas de manera diaria, la cual esta enlazada con la cuenta de correo del administrativo de sistemas.	Administrativo de Sistemas	
3.	**RESTAURACIÓN DE LA INFORMACIÓN:** Iniciar con los procesos de restauración de las carpetas del aplicativo, si por algún motivo el aplicativo PACS llegase a fallar, dañarse o presentar alguna contingencia el administrativo de sistemas, , inmediatamente después de conocidos los hechos el Oficial de Protección de Datos realizará los respectivos reportes a la Superintendencia de Industria y Comercio.	Administrativo de Sistemas Proveedor del Aplicativo	

10.8. Tratamiento de los datos de Servidor Salud IPS y aplicativo DATOS CLINICOS y REPORTES

No.	Actividad	Responsable	Registro
1.	Ingresar al servidor de Salud IP y el aplicativo DATOS CLINICOS y REPORTES está autorizado únicamente para el administrativo de sistemas, el cual genera sus propias copias de seguridad en la carpeta "*Back Up*", las cuales se realizan dos veces al día, a las 12:00 y a las 00:00 respectivamente. La información almacenada en esta carpeta es otorgada por los sistemas internos de la empresa y almacenada en el servidor de información correspondiente.	Administrativo de sistemas	
2.	**COPIA DE SEGURIDAD EN GOOGLE DRIVE:** Programar la sincronización de la carpeta "*Back Up*" en google drive para guardar las copias de seguridad de manera diaria, en la cuenta que esta enlazada con la cuenta de correo del Administrativo de sistemas.	Administrativo de sistemas	
3.	**RESTAURACIÓN DE LA INFORMACIÓN:** Iniciar con los procesos de restauración de la carpeta *"Backup"* del aplicativo y proceder a llamar al proveedor del Sistema para restaurar el aplicativo, si por algún motivo el aplicativo de Salud IPS, o el aplicativo DATOS CLINICOS y REPORTES llega a fallar y/o a dañarse además Inmediatamente después de conocidos los hechos, el Oficial de Protección de Datos realizará los respectivos reportes a la Superintendencia de Industria y Comercio.	Administrativo de sistemas Proveedor del aplicativo	

10.9. Tratamiento de los datos de SISTEMA GESTIÓN DE CALIDAD

No.	Actividad	Responsable	Registro
1.	El acceso al sistema de gestión de calidad se hará mediante la dirección SGC MEDINUCLEAR (192.168.1.77), instalada en todos los computadores de los trabajadores de Medinuclear, donde solo podrán visualizar la información e imprimirla en los formatos requeridos. En ningún momento un trabajador puede editar la información de la carpeta que redirige la dirección IP; las únicas personas que tendrán accedo a editar los documentos serán el gestor de calidad de Medinuclear y el Asistente de calidad.	Gestor de Calidad Asistente de Calidad	
2.	**COPIA DE SEGURIDAD EN GOOGLE DRIVE:** Programar lasincronización de la carpeta *"Back Up"* en google drive para guardar las copias de seguridad de manera diaria, en la cuenta que esta enlazada con la cuenta de correo del administrativo de sistemas.	Administrativo de Sistemas	

11. MEDIDAS DE SEGURIDAD

Conforme a lo expresado en la Política de Tratamiento de Datos Personales de la compañía y en razón a la necesidad de implementar medidas técnicas, administrativas, legales y humanas con el objetivo de mitigar el riesgo de accesos y usos no autorizados o adulteraciones de la información sujeta a tratamiento o uso por parte de MEDINUCLEAR, se citan las siguientes medidas relacionadas con la seguridad en el tratamiento de la información:

11.1. Medidas de seguridad del talento humano.

11.1.1 Reclutamiento y Selección de Personal:

En el proceso de reclutamiento y selección se incluyen, por lo menos, las siguientes actividades en las que se involucra el tratamiento de datos personales.

1) Recepción de hojas de vida de aspirantes:

- Las hojas de vida que se entreguen de manera física o electrónica, (excepcionalmente mediante portales de búsqueda de empleo o bolsas de empleo diferentes) deberán ser custodiadas por el encargado del área de gestión humana del proceso de selección de aspirantes.

- Cuando se trate de hojas de vida físicas, se deben archivar en una carpeta especial, la cual está ubicada en un compartimento específico designado por MEDINUCLEAR, el cual cumple con las condiciones de seguridad que garanticen la confidencialidad de la información.
- La recepción de las hojas de vida, sin excepción del medio en el que se presenten, deberá contar con un acuse de recibo, en el que se deberá incorporar información sobre las finalidades de tratamiento y la remisión a la Política de Protección de Datos Personales.

2) Destrucción de soporte:

- Una vez concluido el proceso de reclutamiento, los documentos físicos y electrónicos de los candidatos que no fueron seleccionados, deberán ser destruidos y podrán conservarse en medio electrónico por un término máximo seis (6) meses por si se requiere contar nuevamente con su información para efecto de una nueva posibilidad de vinculación.
- Los archivos físicos se deberán destruir de manera íntegra y completa, preferiblemente, en una máquina destructora de papel y en ninguna circunstancia podrán ser utilizado como papel reciclable.
- Los documentos digitales, deberán ser eliminados del correo electrónico y del computador, tanto de la carpeta de archivo como de papelera de reciclaje, de la bandeja de entrada del correo electrónico donde se recibió y de la papelera del mismo correo electrónico.
- De igual manera, los documentos que han soportado las diferentes etapas en las que haya participado el candidato, tales como formato de aspirante, soportes de entrevistas, pruebas psicotécnicas y prácticas, formato de visita domiciliaria y valoración global del candidato, deberán destruirse en la misma forma que las hojas de vida y en ninguna circunstancia este material podrá ser reutilizado como papel reciclable.
- Una vez realizada la destrucción de los soportes y documentos se realizará un acta de destrucción.

3) Contratación con terceros:

- En caso de suscribir contratos con fuentes de reclutamiento externas que utilicen datos personales de los aspirantes, se deberá firmar los respectivos acuerdos de tratamiento de datos personales y de confidencialidad que garanticen el adecuado uso de los datos de los titulares.

11.1.2. Vinculación y ejecución del contrato laboral

1) Vinculación:

Una vez seleccionado el candidato y con el objetivo de formalizar su vinculación laboral, este deberá firmar el contrato laboral que debe incluir, mínimo, las siguientes cláusulas:

i. Autorizaciones para el tratamiento de datos personales, de conformidad con la Política de Protección de Datos Personales.
ii. Autorización para el tratamiento de datos sensibles (pertenencia a sindicatos, datos de salud, datos biométricos: huella, fotografía, videograbaciones), sí aplica.
iii. Autorización para el tratamiento de sus hijos menores de edad.
iv. confidencialidad

2) Proceso disciplinario:

Cuando se lleve a cabo un proceso disciplinario con un colaborador, el mismo debe efectuarse conforme a lo estipulado en el Reglamento Interno de Trabajo. Los documentos relacionados con este proceso deben ser conservados de forma que se garantice su acceso y circulación solo a las personas autorizadas.

3) Correo Electrónico y herramientas de colaboración empresarial:

- Las cuentas de correo electrónico y las herramientas de colaboración empresarial de los colaboradores podrán ser monitoreadas en cualquier momento.
- MEDINUCLEAR conserva la propiedad de cada dispositivo y equipo proporcionado a sus colaboradores, en el contexto de su empleo y cargo. El área de sistemas de MEDINUCLEAR será la única responsable de establecer la conectividad de la red de los dispositivos y el acceso a los servicios de red, además de brindar los correspondientes servicios de soporte.
- MEDINUCLEAR se reserva el derecho, a su entera discreción, de exigirle a un colaborador, en cualquier momento, la devolución de todos y cada uno de los dispositivos o equipos que le fueron entregados, incluyendo, sin limitación, en la terminación del contrato laboral. Independiente del motivo o del momento de la solicitud, los colaboradores deben devolver los dispositivo y equipos en buenas condiciones de funcionamiento.
- El uso de los sistemas, equipos y dispositivos está sujeto a la supervisión, monitoreo, auditorías y revisiones por parte de MEDINUCLEAR, con el objetivo de verificar y garantizar un uso adecuado y el cumplimiento de la ley y de las políticas internas de la compañía. Ninguna comunicación transmitida a través de tales sistemas, dispositivos y equipos suministrados por MEDINUCLEAR debe considerarse, en ninguna circunstancia, como privada. MEDINUCLEAR podrá realizar tales auditorias, monitorios y revisiones sin informarle previamente al colaborador.
- MEDINUCLEAR puede utilizar tecnología que le permitirá borrar o destruir de forma remota todos los datos e información contenida en los equipos y dispositivo entregados a sus colaboradores, a través de una conexión inalámbrica. MEDINUCLEAR podrá realizar tal acción en cualquier momento y cada vez que lo considere necesario, por ejemplo: a la terminación del contrato laboral de un colaborador, si el dispositivo o equipo se reporta como perdido o robado, cuando el dispositivo o equipo pueda haber sido comprometido de alguna manera, cuando pueda existir un riesgo real o amenaza de acceso o uso no autorizado del Dispositivo o equipo.

4) Datos Biométricos:

- Toda vez que los datos biométricos son considerados como datos sensibles por la normatividad vigente; cuando se requiera utilizar tecnología biométrica para realizar el tratamiento de los datos de los colaboradores, es necesario contar siempre con el consentimiento explícito del titular de los datos. El consentimiento de los titulares se podrá manifestar (i) por escrito, (ii) de forma oral, o (iii) mediante conductas inequívocas, por ejemplo, a través de señales o avisos que están ubicados de forma visible y legible en las entradas de las instalaciones de MEDINUCLEAR.
- MEDINUCLEAR informará a los titulares de la información el uso de sistemas de videovigilancia; además, informará la ubicación de la política de tratamiento de datos personales y los canales de comunicación mediante los cuales pueden ejercer sus derechos. La finalidad de los sistemas de videovigilancia será la de garantizar la seguridad de las personas y bienes al interior de las

instalaciones de MEDINUCLEAR.

- Las grabaciones e imágenes captadas a través de las cámaras de videovigilancia se conservarán por un término máximo de sesenta (60) días, con excepción de aquellas que el titular de la información o una autoridad competente hayan solicitado su conservación por un tiempo adicional. Las grabaciones e imágenes captadas únicamente se entregarán cuando: (i) sea requerida por una autoridad competente y (ii) la información es solicitada por el titular o representante de quien aparece en la imagen o video; si en la imagen o video aparecen otros terceros titulares de datos personales, el solicitante deberá contar con la autorización de dichos terceros para la entrega de la cinta o grabación.
- El Titular de los datos personales también se encuentra facultado para solicitar la supresión de sus imágenes en la medida que no exista un deber legal o contractual que impida tal supresión, como sería por ejemplo el caso en que los datos personales recolectados mediante una grabación constituyan prueba de la presunta comisión de un delito. Si en la imagen o video aparecen otros terceros titulares de datos personales, el solicitante deberá contar con la autorización de dichos terceros para solicitar la supresión o destrucción de la cinta o grabación.

11.1.3. Uso y conservación

Las siguientes medidas tienes como objetivo garantizar el adecuado manejo y conservación de los datos personales de los trabajadores de MEDINUCLEAR:

- Los documentos del archivo de gestión humana deben guardarse en adecuadas unidades de conservación y almacenamiento, debidamente marcados, sin exposición a humedad, polvo o agentes biológicos que puedan deteriorarlos.
- Los documentos en custodia de gestión humana deberán almacenarse en carpetas debidamente marcadas o rotuladas. Se respetará el nombre asignado al documento en todas las etapas, tales como archivo en gestión, archivo inactivo e histórico, si es del caso.
- El área de gestión humana garantizará un acceso restringido al lugar donde se almacenen la información de tipo personal de los trabajadores de tal manera que se impida el acceso de personas no autorizadas.
- Los archivadores, armarios u otros anaqueles ubicados en el área de gestión humana deberán estar protegidos con llave u otra medida de seguridad que asegure que no se permitirá un acceso no autorizado. Los documentos de carácter confidencial se encontrarán debidamente almacenados en estantes con acceso restringido y con llave.
- La documentación que sea archivada deberá estar en buen estado, completamente depurada, seleccionada, limpia y claramente identificable.
- La consulta de los archivos referentes al reclutamiento, selección, vinculación, hoja de vida del trabajador actual y su desvinculación, solo podrá ser autorizada por el representante legal y el gerente del área de gestión humana de MEDINUCLEAR.
- No se incorporarán datos personales de carácter sensible a la carpeta de los colaboradores más allá de los que puedan llegar a ser necesarios para el cumplimiento de las obligaciones legales del colaborador.
- Cuando se recoja información de tipo sensible, la misma deberá separarse y no deberá ser accesible por personas no autorizadas debido a que la divulgación de este tipo de información puede generar discriminación y acoso al trabajador afectado, además de sanciones por parte de la Superintendencia de Industria y Comercio (SIC) como autoridad colombiana en materia de protección de datos personales.

- Los documentos de carácter confidencial o que contengan información de tipo personal no podrá ser utilizado como papel reciclable, estos documentos deberán ser destruidos con los medios idóneos para garantizar que los mismo no sean reutilizados por ninguna persona al interior de la compañía o algún tercero externo.
- Cuando se determine la eliminación de archivos o destrucción de estos, se deberá destruir de manera tal que impida su recuperación; se sugiere realizar a través de una máquina destructora de papel.
- Cuando se trate de información legal o judicial de un trabajador, como embargos o desembargos, se deberá manejar estrictamente entre el colaborador y quien delegue la gerencia de gestión humana. En ninguna circunstancia la información de este proceso podrá permanecer en los escritorios o quedar expuesta a que un tercero u otro colaborador de MEDINUCLEAR pueda acceder, visualizar o utilizar, sin la debida autorización.

11. 2 Medidas de seguridad del usuario o paciente.

11.2.1 Recepción, uso y archivo de la información

Las siguientes medidas tienes como objetivo garantizar el adecuado manejo y conservación de los datos personales de los clientes, usuarios o pacientes de MEDINUCLEAR:

- Los documentos del archivo de los usuarios o pacientes deben guardarse en adecuadas unidades de conservación y almacenamiento, debidamente marcados, sin exposición a humedad, polvo o agentes biológicos que puedan deteriorarlos.
- Los documentos de los usuarios o pacientes deberán almacenarse en carpetas debidamente marcadas o rotuladas. Se respetará el nombre asignado al documento en todas las etapas, tales como archivo en gestión, archivo inactivo e histórico, si es del caso.
- Las áreas responsables deben garantizar un acceso restringido al lugar donde se almacenen la información de tipo personal de usuarios o pacientes, de tal manera que se impida el acceso de personas no autorizadas.
- Si imprime documentos con información clínica de los usuarios o pacientes, el trabajador debe asegurarse que no queda ningún documento en la bandeja de salida de la impresora.
- Los archivadores, armarios u otros anaqueles que contengan información de los usuarios o pacientes deberán estar protegidos con llave u otra medida de seguridad que asegure que no se permitirá un acceso no autorizado. Los documentos de carácter confidencial se encontrarán debidamente almacenados en estantes con acceso restringido y con llave.
- La documentación de usuarios o pacientes que sea archivada deberá estar en buen estado, completamente depurada, seleccionada, limpia y claramente identificable.
- La consulta de los archivos referentes a las historias clínicas de usuarios pacientes solo podrá ser autorizada por el representante legal y la alta gerencia de MEDINUCLEAR.
- Las historias clínicas de los usuarios o pacientes no deberán ser accesible por personas no autorizadas debido a que la divulgación de este tipo de información puede generar discriminación y acoso; además de sanciones por parte de la Superintendencia de Industria y Comercio (SIC) como autoridad colombiana en materia de protección de datos personales.
- Procurar disminuir la impresión de historias clínicas y documentos relacionados, haciendo uso apropiado de los medios electrónicos y evitando la duplicidad necesaria de la información clínica de los usuarios o pacientes.

- Las historias clínicas o documentos relacionados con la información clínica de los usuarios o pacientes no podrán ser utilizado como papel reciclable, estos documentos deberán ser destruidos con los medios idóneos para garantizar que los mismo no sean reutilizados por ninguna persona al interior de MEDINUCLEAR o algún tercero externo.
- Cuando se determine la eliminación o destrucción de archivos que contengan información clínica de usuarios o pacientes se deberá destruir de manera tal que impida su recuperación; se sugiere realizar a través de una máquina destructora de papel.
- Los documentos que contienen información clínica de los usuarios o pacientes no podrá permanecer en los escritorios de los trabajadores de MEDINUCLEAR o quedar expuesta a que un tercero u otro trabajador pueda acceder, visualizar o utilizar, sin la debida autorización.
- MEDINUCLEAR informará a los usuarios o pacientes el uso de sistemas de videovigilancia; además, informará la ubicación de la política de tratamiento de datos personales y los canales de comunicaciones mediante los cuales pueden ejercer sus derechos. La finalidad de los sistemas de videovigilancia será la de garantizar la seguridad de las personas y bienes al interior de las instalaciones de MEDINUCLEAR.
- Las grabaciones e imágenes captadas a través de las cámaras de videovigilancia se conservarán por un término máximo de sesenta (60) días, con excepción de aquellas que el titular de la información o una autoridad competente hayan solicitado su conservación por un tiempo adicional. Las grabaciones e imágenes captadas únicamente se entregarán cuando: (i) sea requerida por una autoridad competente y (ii) la información es solicitada por el titular o representante de quien aparece en la imagen o video; si en la imagen o video aparecen otros terceros titulares de datos personales, el solicitante deberá contar con la autorización de dichos terceros para la entrega de la cinta o grabación.
- El Titular de los datos personales también se encuentra facultado para solicitar la supresión de sus imágenes en la medida que no exista un deber legal o contractual que impida tal supresión, como sería por ejemplo el caso en que los datos personales recolectados mediante una grabación constituyan prueba de la presunta comisión de un delito. Si en la imagen o video aparecen otros terceros titulares de datos personales, el solicitante deberá contar con la autorización de dichos terceros para solicitar la supresión o destrucción de la cinta o grabación.

11.3 Seguridad operativa y de redes.

Debido a las posibilidades de daño o perdida de la información, resulta necesario definir acciones que permitan proteger los sistemas de información y establecer mecanismos válidos para la gestión de la información. Por lo cual, se han gestionado los siguientes controles de seguridad operativa y de redes para todos los trabajadores de MEDINUCLEAR, según aplique:

1) Cada dispositivo estará bajo la responsabilidad del trabajador al que se le ha sido asignado, quien garantizará que la información a su cargo no pueda ser vista por personas no autorizadas. Los documentos físicos deberán ubicarse en un lugar cerrado y bajo llave que garantice su confidencialidad. Esto aplica para su mesa de trabajo, cualquier tipo de pantalla, impresora u otro tipo de dispositivos conectados a su puesto de trabajo.
2) Cuando el trabajador se ausente de su puesto de trabajo o labor, deberá dejar sus dispositivos o equipos en un estado que imposibilite la visualización de información confidencial, entre estas, la información relacionada con la historia clínica de los pacientes.
3) Cuando las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del archivo impreso, el responsable de cada documento deberá retirar los mismos

conforme se impriman.

4) Cada usuario será responsable de la confidencialidad de sus contraseñas y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá informarlo al área de sistemas y proceder a su cambio.
5) En la gestión de contraseñas, se deberán asignar y cambiar de manera periódica y en especial cuando se presente algún cambio en las condiciones de uso de algunos de los siguientes elementos: hardware, software, elementos físicos de la compañía del cual se deba tener acceso a través de un usuario y contraseña.
6) Cada trabajador es responsable de su equipo de cómputo y deberá ser responsable de su buen estado y el de los demás posibles recursos y software que se le asignen.
7) El uso de correos electrónicos corporativos y herramientas de colaboración empresarial deberán ser usados exclusivamente para fines empresariales de MEDINUCLEAR.
8) Todo trabajador deberá actuar siempre con la debida diligencia, relacionada con el uso y salvaguarda de la infraestructura física y lógica de MEDINUCLEAR, evitando y quedándole prohibido realizar cualquier tipo de acción que vayan en contravía de la sana convivencia, los reglamentos internos y de la ley, entre ellos, pero sin limitarse: actos de acoso, difamación, calumnia, intimidaciones, insultos, tratos hostiles, usos de sistemas tecnológicos para fines personales, pornográficos, discriminatorios o violentos.
9) Está prohibido para cualquier trabajador enviar publicaciones o comunicaciones de cualquier índole como concursos, esquemas piramidales, mensajes en cadena, mensajes no deseados, o cualquier información que no haya sido autorizado por MEDINUCLEAR en razón a sus funciones.
10) El trabajador es el único responsable por el buen uso de su correo electrónico corporativo y de los demás medios o sistemas tecnológicos que MEDINUCLEAR le ha suministrado.
11) Al ausentarse del puesto de trabajo, por ejemplo, descansos, pausas, alimentación, finalización de jornada, deberá dejar completamente libre de documentación su puesto de trabajo.
12) Está prohibido la descarga o instalación de cualquier software de internet u obtenido por otros medios digitales en los computadores corporativos, sin la autorización expresa del área de sistemas.
13) Está prohibido el uso, distribución, reproducción, comunicación, acceso, solicitud, transferencia, publicación, almacenamiento, inducción, provocación, descarga o ejecución de programas clasificados como pornográficos, de juegos, spam, videos, música, imágenes no autorizadas o afines a su labor y la utilización de este tipo de material, ya sea, vía internet o magnética.
14) Está prohibido el uso, distribución, reproducción, comunicación, acceso, solicitud, transferencia, publicación, almacenamiento, inducción, provocación, descarga o ejecución de programas clasificados como obras protegidas por derechos de autor o propiedad industrial, ya sea vía internet o magnética, sin la respectiva autorización.
15) Está prohibido usar herramientas o aplicaciones que comprometan la seguridad de la red de datos, sistemas de información o infraestructura física, si resulta aplicable, que tengan el propósito de realizar cualquiera de los siguientes actos:
    I. Acceder a los sistemas de información o red de datos sin autorización.
    II. Monitorear la red de datos o su tráfico sin autorización.
    III. Atentar de cualquier manera contra los sistemas de información o la red de datos.
    IV. Violar las medidas de seguridad o las reglas de autenticación de los servicios.
    V. Conectarse desde dispositivos móviles externos ajenos a MEDINUCLEAR y sin previa autorización, y que pueda afectar el desempeño de las redes inalámbricas u ópticas.
    VI. Acceder a la red de datos desde dispositivos no autorizados.
    VII. Manipular o alterar software o dispositivos tecnológicos de cualquier índole que

representen un riesgo para MEDINUCLEAR y que no haya sido autorizado.

VIII. Intentar o borrar, eliminar, modificar, o alterar cualquier tipo de información de MEDINUCLEAR sin importar el formato en el que se encuentre y sin la debida autorización expresa para ello.

16) La información confidencial o critica debe utilizarse en carpetas destinados para tal fin, realizando siempre las respectivas copias de seguridad y el respectivo respaldo de la información.
17) En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, especialmente si está siendo transportado en un vehículo.
18) Está prohibido ingerir cualquier tipo de alimento o bebidas cerca de dispositivos tecnológicos o elementos físicos suministrados por MEDINUCLEAR.
19) Los usuarios de los equipos de cómputo de MEDINUCLEAR deben mantener una copia de respaldo (copia de seguridad) de toda la información estratégica e importante. Para este fin, deben consultar al área de sistemas sobre la mejor manera de llevar a cabo esta copia de respaldo.
20) Todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red corporativa, cuando esto aplique.
21) Con el fin de minimizar los riesgos de seguridad de los sistemas de información, solo permite la instalación de aplicaciones y sistemas operativos que cuenten con una licencia de software libre o una licencia propietaria y previamente autorizado por el área de sistemas. Además, no se permite el uso de versiones de software que no sean soportadas por los fabricantes.
22) Las unidades de medios removibles deben estar deshabilitadas en los servidores y equipos de cómputo. En caso de ser necesario el uso de medios removibles, se debe solicitar la autorización previa del área de sistemas y hacer seguimiento a la transferencia de la información a estos medios.
23) Cualquier software que tenga la capacidad de comprometer un dispositivo, equipo o los datos de MEDINUCLEAR podrá generar que el respectivo equipo o dispositivo sea bloqueado, eliminado administrativamente o cancelado su servicio por completo, a discreción del área de sistemas de MEDINUCLEAR.
24) Los dispositivos o equipos no deben modificarse de ninguna manera que afecte la seguridad o la garantía del dispositivo.

11.4. Gestión de los sistemas de información.

En caso de algún cambio relativo con los sistemas de gestión de la información, MEDINUCLEAR hará un llamado a los trabajadores y contratistas a notificar de dichos cambios con el fin de tomar las respectivas decisiones al respecto, entre estas, las siguientes:

- El abordaje y control completo de la situación de cambio.
- El diagnóstico, análisis, evaluación y seguimiento de los riesgos y medidas a tomar.
- La respectiva formulación o reformulación de textos contractuales relacionados con los contratistas o proveedores de la compañía.
- Realización de las respectivas matrices de riesgo.

Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado

adecuadamente por el área de sistemas; además, debe ser sometido a una evaluación que permita identificar riesgos asociados que pueden afectar las bases de datos y la operación del negocio, de acuerdo con los lineamientos de gestión de cambios. El respectivo procedimiento debe contener como mínimo la identificación, justificación y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica, el alcance, autorización, el plan de trabajo para la definición de pruebas funcionales, responsabilidades definidas, la evaluación apropiada sobre el impacto potencial que estos puedan generar, un plan alternativo para abortar cambios no satisfactorios, eventos imprevistos y cualquier otro aspecto que se considere importante por los responsables del cambio.

11.5. Gestión de la relación con proveedores.

En los contratos de prestación de servicios y demás contratos de cualquier tipo que celebre MEDINUCLEAR con terceros que impliquen el tratamiento de datos personales, se realizará la transmisión con el encargado del tratamiento de datos y, en lo posible, sus contratos incluirán cláusulas que precisan los fines, medios, medidas de seguridad aplicables y tratamientos autorizados por MEDINUCLEAR y delimitará de manera precisa el uso que estos terceros le pueden dar a aquellos, así como las obligaciones y deberes establecidos en normatividad aplicable, incluyendo las medidas de seguridad necesarias que garanticen en todo momento la confidencialidad, integridad y disponibilidad de la información de carácter personal encargada para su tratamiento.

Cuando MEDINUCLEAR reciba datos de terceros y actúe como encargado del tratamiento de datos de carácter personal, verifica que la finalidad, o finalidades de los tratamientos autorizados por el titular o permitidos por causas legales, contractuales o jurisprudenciales se encuentran vigentes y que el contenido de la finalidad esté relacionada con la causa por la cual se va a recibir dicha información personal de parte del tercero, confirmando la facultad para recibir y tratar dichos datos personales.

Cualquier tipo de información obtenida o tratada por MEDINUCLEAR a través de cualquier formato, físico o electrónico, contrato, comunicación, física, electrónica o telefónica, entre otros, serán tratados con total reserva y confidencialidad, comprometiéndose a guardar el debido secreto respecto de los mismos y garantizando el deber de almacenarlos adoptando medidas necesarias que eviten su alteración, pérdida y tratamiento o acceso no autorizado, de acuerdo con lo establecido en la legislación aplicable.

11.6 Protección de las contraseñas personales.

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos e información personal, por lo cual, deben estar especialmente protegidas. Como “llaves” de acceso a los sistemas de MEDINUCLEAR, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al área de sistemas y subsanada en el menor plazo de tiempo posible.

Por lo tanto, cada usuario será responsable de la confidencialidad de sus contraseñas y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá informarlo al área de sistemas y proceder a su cambio. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad, determinados por el área de sistemas.

12. CUMPLIMIENTO.

Todos los miembros de MEDINUCLEAR serán responsables de implementar las políticas y procedimientos de seguridad que se contemplan o son referenciados en este documento y sus complementarios. Toda conducta de cualquier miembro de MEDINUCLEAR que no respete o acate las consideraciones del presente Manual será considerado como un incumplimiento a las políticas de la compañía; entre los ejemplos de incumplimiento se incluyen, pero sin limitarse a ellos, los siguientes:

- Negligencia en la aplicación de medidas de seguridad y control.
- No comunicar inmediatamente al oficial de protección de datos o al área de sistemas los problemas de seguridad de la información que sean detectados.
- No tomar las medidas correspondientes ante una queja o un incidente de seguridad.
- Comunicar a terceros datos personales de las bases de datos de MEDINUCLEAR, sin estar previamente autorizado para ello.

Cualquier incumplimiento de las políticas y procedimientos de seguridad será considerado como falta disciplinaria por incumplimiento de las obligaciones y deberes del trabajador; la cual podrá será sancionada según corresponda y de acuerdo con la gravedad de la infracción. Entre las sanciones, MEDINUCLEAR podrá proceder con la terminación del contrato de trabajo con justa causa, suspensión del contrato o amonestación escrita con copia a la hoja de vida, atendiendo las circunstancias particulares de cada caso de conformidad con lo previsto en la Ley. Los colaboradores temporales, proveedores y otros terceros que estén involucrados en incidentes de incumplimiento pueden ver terminado su contrato con justa causa sin que esto implique el pago de indemnizaciones, perjuicios o expectativas económicas.

13. INDICADORES

N/A

14. BIBLIOGRAFIA:

N/A

15. ANEXOS:

N/A