INSTITUTO NEUMOLÓGICO DEL ORIENTE SA

POLÍTICA SEGURIDAD DE LA INFORMACIÓN

BUCARAMANGA- COLOMBIA

ACTUALIZACIÓN: 24-MAY-2024

CÓDIGO: INF-O-02, v:02

POLITICA SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Establecer los mecanismos para garantizar la seguridad y confidencialidad en el uso de la información y los recursos tecnológicos.

2. ALCANCE

La presente política de seguridad de la información debe ser conocida y cumplida por todos los colaboradores del Instituto neumológico del oriente. Sin importar la jerarquía del cargo

3. RESPONSABILIDADES

- Personal del Instituto Neumológico del Oriente
- Coordinadora de Gestión de la Información.

4. DOCUMENTOS DE REFERENCIA

- ISO 27000 (TODA LA SERIE).

- LEY 1273 DE 2009: protección de la información y de los datos.

5. DEFINICIONES

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas Personas autorizadas a tener acceso a la misma.
- **Integridad**: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- **Disponibilidad**: garantiza que los usuarios autorizados tengan acceso a la Información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Información**: Se refiere a toda comunicación o representación de conocimiento como Datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, Cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en Papel, en pantallas de computadoras, audiovisual u otro.
- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de Información organizada para la recopilación, procesamiento, mantenimiento, Transmisión y difusión de información según determinados procedimientos, tanto Automatizados como manuales.
- **Tecnología de la Información:** Se refiere al hardware y software (equipos, teléfonos, impresoras etc) operados por la organización o por un tercero que procese información en su nombre, para llevar a cabo Una función propia de la organización, sin tener en

cuenta la tecnología utilizada, ya se Trate de computación de datos, telecomunicaciones u otro tipo.

- **Backups:** Es una copia de seguridad o el proceso de copia de seguridad. Backups se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- **Computador:** es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU
- **Gusano**: virus o programa auto replicante que no altera los archivos, sino que reside en la memoria y se duplica a sí mismo.
- **Incidente de seguridad:** es cualquier evento que daña o representa una amenaza seria para toda o una parte de la infraestructura y tecnología del INO., pueden ser. Ausencia de servicios, inhibición para el uso de sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos, delitos definidos en la Ley 1273 de 2009.
- **Sistema Operativo**: Plataforma operativa, programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.
- **Software:** todos los componentes no físicos de una PC (Programas).
- **Usuario:** toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

6. CONDICIONES GENERALES

- Todo funcionario nuevo en el Instituto Neumológico del Oriente, deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, donde se dan a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

- El INSTITUTO NEUMOLÓGICO DEL ORIENTE, está comprometido con la preservación de la confidencialidad, disponibilidad e integridad de la información de la institución, así mismo, se compromete con la protección de los bienes de la información contra uso, modificación, acceso o destrucción no autorizada.

7. DESCRIPCIÓN

A continuación, se encuentran las normas que debe conocer y cumplir todo colaborador del instituto Neumológico del Oriente, en relación con el uso de los recursos de información de la Empresa como: computadores personales, servidores, impresoras, sistemas de información, redes, manuales, software y sus licencias, y correo electrónico, Internet, información, entre

otros. Su incumplimiento podrá conllevar sanciones administrativas y/o las contempladas en la legislación colombiana.

7.1 NORMAS BÁSICAS

- Utilizar con criterios de racionalidad los sistemas y recursos de información del instituto neumológico del oriente. Solamente para llevar a cabo el objeto del negocio de la empresa o labores propias de su función. Su uso estará sujeto a verificaciones cuando el Instituto neumológico del oriente lo considere conveniente.

- Dar manejo a la información de acuerdo con los criterios de confidencialidad, disponibilidad e integridad ya mencionados y que fueron socializados con su contrato de trabajo.

- Los mecanismos de seguridad previstos en las aplicaciones o correo electrónico como son el usuario (o cuenta) y su contraseña, son de carácter único, personal e intransferible. Por tanto, cualquier acción realizada con esta cuenta será responsabilidad de la persona a quien se le entregó esta información. En razón con lo anterior, agradecemos seguir las recomendaciones presentadas en este documento.

7.2 CONTROL DE ACCESO A LA INFORMACION

Dada la importancia que tiene el acceso a la información del instituto neumológico del oriente a continuación se dan las pautas para crear contraseñas de manera segura, confiable y evitar que personas no autorizadas tengan acceso a los sistemas de información.

- No utilizar contraseñas que sean fáciles de deducir o palabras obvias.
- La contraseña debe tener una longitud mínima de ocho caracteres.
- La contraseña debe estar compuesta por caracteres alfanuméricos y especiales.
- Debe memorizarlas.
- No compartirla.
- Cambiar la contraseña cada 30 días.
- Evitar reciclar viejas contraseñas.
- No utilizar combinaciones obvias de teclado, como por ejemplo “1q2w3e4r”.
- No utilizar claves secuenciales, como YU78WE01, YU78WE02, o ‘qwerty’.
- Utilizar una de las siguientes reglas para su creación: Seleccionar una frase común y tomar la primera o última letra de cada palabra, por ejemplo: Con la frase “En el universo ninguna deuda queda pendiente”, siendo la palabra clave: Eeundqp.

Seleccionar las consonantes de una palabra en orden establecido por el usuario y agréguele algunos números. Ejemplo: Palabra crucigrama, palabra clave: crcgrm09.
Seleccionar dos palabras y unirlas por caracteres especiales. Ejemplo: mi$mascota.

Nota: Al ingresar a la organización se asignan permisos básicos para el acceso al sistema de información. El coordinador o líder de área es la persona a cargo de solicitar permisos AVANZADOS en los sistemas de información cuando los colaboradores los requieran.

7.3 MEDIOS DE COMUNICACIÓN (Vozip)

Para dar respuesta a las necesidades de comunicación que se puedan presentar a los colaboradores del instituto neumológico del oriente, ha dispuesto de la tecnología de comunicaciones vozip. Los colaboradores podrán entablar comunicación entre las diferentes sedes de la organización y procesos a través de uso de teléfonos y la marcación de extensiones telefónicas. También se ha implementado la plataforma de correo electrónico con el fin de que los colaboradores puedan hacer uso de los servicios de mensajería electrónica, chat en línea y servicios video conferencia.

Para acceder a los permisos de minutos a larga distancia o llamadas a líneas de celulares el coordinador o líderes de área deberá realizar la solicitud a gestión de la información a través del software de mesa de ayuda. Es responsabilidad del colaborador utilizar este servicio solo para las funciones asignadas. La tecnología Vozip tiene una herramienta para el monitoreo del uso del servicio con fines de garantizar la calidad en la prestación del mismo.

La telefonía implementada en la organización permite la grabación y almacenamiento de la voz con el fin de garantizar un buen servicio. Las grabaciones de voz solo se entregarán a lideres y coordinadores de área. No se entregará información de la plataforma de telefonía directamente a ningún colaborador o tercero.

7.4 USO DE LA PLATAFORMA MESA DE AYUDA

Se estableció la plataforma mesa de ayuda para que los colaboradores reporten las necesidades de soporte de sistemas de información y de comunicaciones e información al proceso de gestión de la información. Todas las solicitudes de soporte técnico deben registrarse a través de la aplicación GLPI con el fin de que se garantice la oportunidad en la atención.

Los tiempos de atención para la solución de las solicitudes reportadas a través de la mesa de ayuda son:

Minutos	Horas	Urgencia
480 Min	8 Hora	Alta
720 Min	12 Horas	Mediana
4320 Min	72 Horas	Baja

Los permisos avanzados en el acceso a la información y las comunicaciones deben ser reportados al coordinador o líder de proceso quien es la persona autorizada para realizar la solicitud. Cuando no se pueda dar respuesta a las solicitudes registradas en la mesa de ayuda por el colaborador; el proceso de gestión de la información le informará a través de correo electrónico el impedimento por el cual no se le podrá dar respuesta.

Es responsabilidad del colaborador reportar las incidencias que tenga a través del software de mesa de ayuda. Si ha utilizado otros métodos de reporte no serán válidos para el proceso de gestión de la información ya que la mesa de ayuda es la única herramienta aprobada institucionalmente.

7.5 ASIGNACIÓN DE RECURSOS

El proceso de gestión de la información está a cargo de hacer entrega de recursos de información, sistemas y comunicaciones como son: teléfonos, impresoras, computadores, diademas, mouse, teclados etc. Cuando los colaboradores requieran algún tipo de recurso para la ejecución de las funciones asignadas deberán comunicar inicialmente la solicitud al coordinador o líder de proceso. El líder coordinador o líder es el responsable de gestionar la solicitud a través de la plataforma Glpi ante el proceso de gestión de la información y proceso de compras.

7.6 IMPRESIÓN DE INFORMACIÓN CONFIDENCIAL

En el instituto se ha establecido la impresión de documentos con información confidencial. Se sugieren las siguientes recomendaciones para garantizar que la impresión se realice de forma segura y que no se viole el principio de la confidencialidad:

- Imprima información confidencial solo en áreas de acceso controlado.
- Imprima información confidencial donde la impresora sea atendida de forma personal.
- Si ninguna de estas opciones no está disponible en el lugar donde se encuentra, puede utilizar una impresora localizada en área abierta siempre y cuando la recoja inmediatamente la envía.

7.7 SEGURIDAD EN EQUIPOS FÍSICOS (HARDWARE)

El instituto neumológico del oriente realizara entrega de la tecnología necesaria para la ejecución de las funciones de los colaboradores. El colaborador es responsable de brindar los cuidados necesarios para garantizar el correcto uso de la tecnología asignada. Cuando se identifique mal uso de los equipos tecnológicos se realizará procedimiento a través del proceso de gestión humana para identificar responsabilidades y sanciones.

Se recomienda a todos los colaboradores reforzar permanentemente las medidas de protección física de los equipos o elementos que utilice o de los cuales sea custodio. No descuidarlos ni exponerlos a pérdidas o hurtos, es responsabilidad de cada colaborador y/o, contratista:

- Bloquear los equipos de cómputo cada vez que se retire o deje su estación de trabajo desatendida.
- No consumir alimentos en el puesto de trabajo.
- No Trasladar o mover los equipos sin autorización del coordinador de proceso y el proceso de gestión de la información y compras.
- Cuando utilice su equipo portátil en instalaciones diferentes del instituto neumológico del oriente, verifique que las condiciones eléctricas son las requeridas por los fabricantes de su equipo.
- No utilizar el equipo de cómputo ante la identificación de un daño parcial o total o ante la sospecha de virus.
- Realizar la solicitud de verificación de los equipos ante presencia de virus y mal funcionamiento del equipo a través de la plataforma Glpi.
- No abrir directamente o permitir a otras personas abrir los equipos, extraer, manipular y/o cambiar sus partes.
- No golpear o utilizar descuidadamente o inadecuadamente los equipos.
- No Exponer los equipos a mecanismos de control que puedan dañar sus partes o su información (Ejemplo: detector de metales y rayos X entre otros).
- Mantener actualizado el inventario de hardware y software que esté bajo su responsabilidad y verificar las condiciones de los equipos y del software antes y después de cada mantenimiento o de cada visita o intervención del personal técnico, del mismo modo acompañar al técnico mientras se realicen este tipo de procedimientos.
- Cumplir con los procedimientos de traslado, trasferencia o entrega de equipos activos informáticos de las instalaciones del instituto neumológico del oriente.
- Al retirarse de la Empresa, hacer entrega formal de los recursos asignados, incluyendo, hardware, software e información, entre otros, al responsable del proceso y a su vez a la coordinación del proceso de gestión de la información.
- Utilizar los equipos tecnológicos solo con fines laborales

Recomendaciones al abandonar su área de trabajo o al final del día:

- Apague su estación de trabajo (equipo de cómputo, tableta, iPad etc).
- Cierre su oficina si trabaja en una oficina cerrada. Verifique la seguridad.
- Si utiliza un computador portátil y desea dejarlo en su área de trabajo, asegúrelo con la guaya en el escritorio o déjelo en un cajón con llave. Si no tiene Guaya solicítela al proceso de compras y gestión de la información.
- Ningún colaborador deberá extraer equipos de cómputo después de finalizada su jornada laboral. Si requiere extraer el equipo de cómputo de las instalaciones, deberá ser autorizado por su jefe directo y por tanto el colaborador asumirá la responsabilidad de perdida, daño o hurto. Igualmente, el colaborador deberá verificar antes de retirar el equipo de cómputo, que se dé cumplimento a su proceso de copias de seguridad.

7.8 LICENCIAMIENTO

Los colaboradores solo podrán utilizar software legalmente adquiridos por el instituto neumológico del oriente., sin copiar o duplicar software licenciado, excepto cuando es explícitamente permitido en los términos y condiciones de la licencia. Si el colaborador requiere instalar un software específico, debe contar con la aprobación formal del coordinador o líder del proceso de gestión de la información, área que analizará las implicaciones a nivel de la licencia y uso que este software pueda tener en la infraestructura de TI y soluciones de información. En caso de presentarse algún tipo de reclamación por software ilegal, ésta recaerá sobre el colaborador responsable del activo en el que se encontrase dicho software.

Dado lo anterior el usuario del software no deberá:

- Copiar, vender, regalar, distribuir el software o su documentación sin permiso del autor.
- Estimular, permitir, obligar o presionar a los empleados a crear o utilizar copias no autorizadas.
- Prestar los programas para que sean copiados, o copiar los programas que han sido pedidos en préstamo.
- Ejecutar un programa en dos o más computadores simultáneamente, a no ser, que esté específicamente permitido en la licencia.
- Alterar, modificar o adaptar el software y la documentación, incluyendo entre otras acciones la traducción, ingeniería reversa del código, desensamblado o creación de trabajos derivados.
- Utilizar hardware o software de monitoreo de actividades (analizadores de protocolos, software catalogado como “hacking”, etc.) sin la debida autorización.

7.9 DERECHOS DE AUTOR

En la terminología jurídica, la expresión "derecho de autor" se utiliza para describir los derechos de los creadores sobre sus obras literarias y artísticas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los **programas informáticos**, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos.
Se incurre en delito por:

- El uso inapropiado de información de terceros, protegidos por el derecho de propiedad intelectual.
- La apropiación y reproducción indebida de información sin citación de la fuente.
- Si estas cosas se hacen en el ámbito laboral, se está comprometiendo a la organización y al funcionario en dicho ilícito.
- No copie, ni todo ni en partes, libros, artículos, programas, reportes y otros documentos, que no estén permitidos por la ley de derecho de autor.

ACCESO A LA RED INTERNA DEL INSTITUTO NEUMOLOGICO DEL ORIENTE

Gestión de la información es el encargado de brindarle acceso a las redes de la organización para que el colaborador pueda ejecutar sus funciones. Se recomienda
No utilizar las redes del instituto neumológico del oriente para conectar dispositivos PERSONALES como: tabletas, Smartphone, equipos de cómputos etc. Que no pertenezcan a la organización.
Para el acceso de nuevos equipos a la red de la organización se debe realizar la solicitud a través de Glpi.

7.10 CONEXIONES EXTERNAS Y DE ACCESO REMOTO

Por ser un riesgo potencial cada conexión entre la red y los sistemas del Instituto neumológico del oriente o redes externas serán estrictamente controlados y deben ser aprobados por la coordinación del proceso de gestión de la información.

Para conectarse a redes o sistemas internos del instituto neumológico del oriente, fuera de las instalaciones de la empresa, debe tener la aprobación del coordinador o líder de gestión de la información para el uso de acceso remoto.

Los colaboradores no están autorizados para brindar accesos remotos a personas ajenas a la organización (proveedores, ingenieros, contratistas etc). El colaborador que permita u conexiones remotas será responsable de las incidencias que pudieran ocurrir al fallar la seguridad de la red.

7.11 USO DE INTERNET

El acceso a los servicios de internet es limitado en la organización. Si se requiere del servicio de internet avanzados; los colaboradores deben notificar la necesidad inicialmente al coordinador y líder de proceso. El coordinador o líder debe realizar la solicitud de acceso a este servicio a través de la mesa de ayuda a gestión de la información, especificando el tipo de permiso que requiere.

Aun cuando se habiliten los permisos de internet avanzado; no se autoriza el uso del internet para ingreso a páginas que generen tiempos de ocio ya que esta herramienta está habilitada solo para el uso de labores institucionales asignadas al colaborador.

7.12 USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

El uso del correo electrónico es estrictamente laboral. Los permisos de acceso a la cuenta de correo se establecerán desde el ingreso a la organización. El colaborador debe cumplir con las siguientes recomendaciones:

- No enviar correo a nombre de otra persona
- No enviar propaganda no solicitada vía correo.
- No enviar o responder a cadena de mensajes o correos masivos sin autorización
- No utilice Internet (cuentas de Hotmail, yahoo, etc.) para enviar correos del instituto neumológico del oriente a otro funcionario. Siempre utilice las facilidades del correo interno.
- Utilizar la cuenta de correo interno del instituto neumológico del oriente. para enviar y recibir única y exclusivamente correos relacionados con su área de trabajo. Para él envió de correos personales, puede utilizar sus cuentas de correos gratuitas (cuentas de Hotmail, yahoo, Gmail etc.).

Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

7.13 CÓDIGO MALINTENCIONADO Y DAÑINO

Debe verificar el tipo de software que instala y ejecuta en sus equipos de trabajo, así como los sitios web que visita, ya que estos sistemas pueden contener códigos maliciosos que desencadenan acciones de espionaje, borrado de archivos, infección y bloqueo de las funcionalidades del equipo. Dichos “códigos o virus”, generalmente se ejecutan de forma silenciosa.

Los colaboradores deben informar a gestión de la información cuando identifiquen que existe algún tipo de riesgo o fallas en los sistemas de información y la tecnología.

7.14 SITIOS WEB NO APROPIADOS

En el instituto neumológico del oriente se tiene limitados el uso de internet a través de reglas de acceso. Cuando requiera acceder a sitios web que no corresponden a la actividad del instituto. ni a las funciones asignadas a su cargo y que sean requeridos por una razón justificada, el coordinador de área o líder de proceso deberán realizar la solicitud a través de la mesa de ayuda

Ejemplos de sitios que requieran aprobación justificada:

- Sitios Web que contienen descarga de música o videos.
- Sitios Web que contienen imágenes y material explícito pornográfico.
- Sitios Web que promueven actividad ilegal.
- Sitios Web que promueven la intolerancia, ejemplo: con contenido racista

7.15 USO DE REDES SOCIALES EN LA ORGANIZACIÓN

El establecimiento de una política de uso de redes sociales busca que los empleados las manejen con el criterio adecuado, con sentido común, y que sus publicaciones a título personal o corporativo no comprometan a la empresa en situaciones problemáticas e innecesarias. Es política organizacional:

- No realizar publicaciones en redes sociales que comprometan el nombre de la organización.
- No realizar publicaciones en redes sociales con imágenes de pacientes o procesos de atención que vulneren los derechos del mismo y de su familia.
- No publicar información de la organización, del paciente o de la familia del paciente en redes sociales.
- No crear sitios web blogs, fanpage, cuentas en Facebook u otras redes a nombre del instituto neumológico del oriente si no está autorizado por Gerencia.

7.16 ESCRITORIO Y PANTALLA LIMPIA

Para garantizar la seguridad y confidencialidad de la información los colaboradores deben:

Mantener los puestos de trabajo limpios de documentos. Los documentos deben estar guardados en áreas seguras. Se debe mantener el escritorio o fondo de pantalla del equipo limpio de información. Se debe hacer uso de la unidad de almacenamiento mis documentos o el almacenamiento el Work Drive.

7.17 CIRCUITO CERRADO DE TELEVISIÓN

Se ha implementado en la organización la grabación de video a través del circuito cerrado de televisión con el objetivo de garantizar la seguridad de las instalaciones. Gestión de la información podrá verificar la información almacenada en los dispositivos solo si existe autorización de un coordinador o líder. No se entregará información del CCTV directamente a ningún colaborador o tercero.

7.18 INGRESO DE PROVEEDORES CONTRATISTAS Y TERCEROS

Es política que todas las personas ajenas a la organización ingresen con previo acompañamiento de un líder o coordinador de área con el fin de prevenir riesgos o eventos que perjudiquen el funcionamiento de los procesos, de la organización o de los pacientes.

Personas ajenas a la organización no pueden realizar modificaciones en los sistemas de información ni a las tecnologías informáticas sin previa autorización del líder o coordinador del proceso.

Los cambios a los sistemas o la tecnología informática son controlados a través del proceso de gestión de la información (sistemas) por lo que los cambios serán informados con anticipación al líder o coordinador del proceso con el fin de coordinar los tiempos de parada.

Los colaboradores no están autorizados para solicitar cambios o modificaciones a los sistemas de información y/o tecnología informática a proveedores, contratitas o terceros.

Los colaboradores deben manifestar todas las necesidades a través de la herramienta establecida por la mesa de ayuda (GLPI) para brindar soporte.

Los eventos o incidentes que se presenten en los procesos por cambios a la tecnología o a los sistemas de información sin previa autorización del proceso de gestión de la información deberán ser asumidos por el colaborador que permitió el acceso y/o modificación. Se recomienda no asumir este riesgo.

7.19 COPIAS DE SEGURIDAD

El instituto neumológico del oriente a dispuesto de herramientas y metodologías de control para realizar copias de seguridad a los equipos de cómputo de los colaboradores.

Es responsabilidad del colaborador velar por el cumplimiento de ejecución de copia de seguridad del equipo asignado.

Es responsabilidad del colaborador almacenar en el equipo de cómputo solo información que corresponda al ámbito laboral por lo que se prohíbe guardar información como son: películas, música, fotos, videos que no hagan parte de las funciones del colaborador.

7.20 PREVENGA EL CONTAGIO DE VIRUS

- No utilice dispositivos USB. Si los va a utilizar realice escaneo con el antivirus institucional antes de abrirlos.
- No permita que personas ajenas a la organización utilicen su equipo de cómputo.
- No permita que a su área de trabajo ingresen personas ajenas a la institución a manipular los equipos y/o sistemas de información.
- No conecte los equipos tecnológicos a redes diferentes a las del instituto neumológico del oriente
- Ejecute las actualizaciones que le pide el sistema operativo.
- Informe inmediatamente si sospecha de infección con virus a la mesa de ayuda.

Ante el incumplimiento a las políticas anteriormente mencionadas, se establecerán sanciones a través del proceso de gestión humana por lo que es importante que, si no comprende la información anteriormente, solicite mayor información al proceso de gestión de la información.

7.21 PÉRDIDA DE EQUIPO

Los colaboradores que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia.

El funcionario deberá dar aviso inmediato a su líder inmediato y a la administración de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

7.22 INFORMACIÓN SENSIBLE Y/O CONFIDENCIAL

Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Instituto Neumológico del Oriente.

La información almacenada en los equipos de cómputo del Instituto, es propiedad del INO y cada usuario es responsables por proteger su integridad, confidencialidad y disponibilidad.

Toda información en formato electrónico o impreso del INO, debe estar debidamente identificada, ya sea a través de rótulos o etiquetas, lo que permitirá su identificación y clasificación.

7.23 CONTROLES PARA OTORGAR, MODIFICAR Y RETIRAR ACCESOS A USUARIOS

La creación, modificación y eliminación de usuarios en las respectivas plataformas del INO, estarán a cargo del responsable de gestión de la información junto con el proceso de gestión humana quien notificara a través de correo electrónico el retiro o ingreso del colaborador.

Para la desactivación de los usuarios el proceso de gestión humana debe entregar a gestión de la humana la paz y salvo del colaborador

7.24 GESTIÓN DE INCIDENTES

Se llevará control detallado de los incidentes de seguridad de la información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

Cualquier dispositivo de uso personal como teléfonos inteligentes, computadores portátiles, tabletas u otros dispositivos de cómputo que estén implicados en incidentes de seguridad pueden ser sometidos a cadena de custodia o protección para fines de investigación o evidencia ante procesos administrativos o legales.

Los reportes de incidentes deben ser ejecutados y controlados por la empresa de Telecomunicaciones, junto con el apoyo del coordinador de gestión de la información.

DISPOSICIONES FINALES

INSTITUTO NEUMOLÓGICO DEL ORIENTE SA designa a El personal del área administrativa y asistencial como Responsable de la adopción e implementación de las obligaciones previstas en la Ley 1581 de 2012.

PERSONA O ÁREA RESPONSABLE DE LA PROTECCIÓN DE DATOS PERSONALES:

INSTITUTO NEUMOLÓGICO DEL ORIENTE SA designa personal del proceso administrativa y de sistemas de información, o quien haga sus veces, para cumplir con la función de la seguridad de la información.

8. REVISIÓN DEL DOCUMENTO

POLITICA SEGURIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS					
Versión	**Fecha**	**Control Documental**	**Nombre**	**Cargo**	**Descripción del Cambio**
02	24/05/2024	Elaboró	Diana Patricia Pérez	Líder Gestión de la Información	Se ajusta la estructura del documento de acuerdo al Proyecto Almera en fase de inicio.
		Revisó	Doris Calderón Rojas	Profesional de Sistemas de Gestión	
		Aprobó	Leidy Marcela Villabona Rodríguez	Líder sistemas de Gestión	