INSTITUTO DE GASTROENTEROLOGÍA Y HEPATOLOGÍA DEL ORIENTE COLOMBIANO S.A.S

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS INFORMÁTICOS

Código: PR-01GIN-02 Versión: 00

Elaborado por	Diana Maria Caceres Uribe Administradora		
REVISIONES Y APROBACIONES			
N°	**Nombre**	**Cargo**	**Firma**
01	Diana Maria Caceres Uribe	Administradora	
02			
03			
04			
Aprobado por	Dr. Elmer Jair Ruiz Lobo Gerente		
20/12/2015 Fecha de Elaboración	23/12/2015 Fecha de Aprobación	10/09/2016 Fecha de Próxima Revisión	

CONTROL DE APROBACIONES Y REVISIONES

No	Fecha	Motivo de revisión
00	23/12/2015	Liberado

INTRODUCCIÓN

Descripción del alcance del documento y breve explicación o resumen del mismo. También se puede explicar algunos antecedentes que son importantes para el posterior desarrollo del tema central. El lector al leer la introducción debería poder hacerse una idea sobre el contenido del documento, antes de comenzar su lectura propiamente dicha. Puede incluir una o más subsecciones estándar, como lo son el resumen o síntesis, el prefacio y los agradecimientos

JUSTIFICACIÓN

La masiva utilización de recursos informáticos (Computadores, impresoras, redes de datos, etc.) como medio para almacenar, transferir y procesar información, se ha incrementado desmesuradamente en los funcionamiento de la sociedad y de las diferentes Empresas.

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 empresa no puede ser indiferente 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 ley.

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.

1. OBJETIVOS

- Se describen los logros que queremos alcanzar con la ejecución de una acción planificada. Los objetivos deben expresarse con claridad para evitar posibles desviaciones y ser susceptibles de alcanzarse. Deben ser concretos, claros, realistas y modestos, en la medida en que realmente reflejan la contundencia de quien elabora el documento en su intención de aportar en el conocimiento del objeto de estudio

2. MARCO CONCEPTUAL

Administrador del sistema: Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está en cabeza de la Dirección Administrativa

Administrador de correo: Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros usuarios en un servidor.

Buzón: También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la empresa.

Chat: (Tertulia, conversación, charla). Comunicación simultanea entre dos o más personas a través de internet.

Computador: Es un dispositivo de computación de sorpresa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

Contraseña o password: Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Correo electrónico: También conocido como E-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

Cuenta de correo: Son espacios de almacenamiento en un servidor de correo, para guardar información de correo electrónico. Las cuentas de correo se componen de un texto parecido a este aaaaaa@ighosas.com donde "aaaaaa" es nombre o sigla identificadora de usuario, "ighosas" el nombre de la empresa con la que se crea la cuenta o el dominio y ".com" una extensión propia de Internet según el dominio.

Edición de cuentas de correo: Mirar o leer el contenido de los correos recibidos o enviados por un usuario.

"La información contenida en el presente procedimiento es propiedad de IGHO SAS es SECRETA Y CONFIDENCIAL. Las personas que lo reciben son responsables por su seguridad y prevención del uso indebido"

Downloads: Descargar, bajar. Transferencia de información desde internet a una computadora.

Electricidad Estática: La corriente estática se presenta cuando no existe ninguna fuerza externa (voltaje) que impulse a los electrones o si estos no tienen un camino para regresar y completar el circuito, la corriente eléctrica simplemente "no circula". La única excepción al movimiento circular de la corriente la constituye la electricidad estática que consiste en el desplazamiento o la acumulación de partículas (iones) de ciertos materiales que tienen la capacidad de almacenar una carga eléctrica positiva o negativa.

Elementos de tecnología: Se consideran los siguientes, elementos como activos tecnológicos.

- Computadores de escritorio y portátiles: conformados por CPU (Discos duros, memorias, procesadores, main borrad, fuente de poder, bus de datos), cables de poder, monitor, teclado, mouse.
- Impresoras, UPS, escáner, lectores de DVD , fotocopiadoras, teléfonos, radioteléfonos.
- Equipos de redes comunicaciones como: Swithc, router, Hub, Conversores de fibra y demás equipos de redes y comunicaciones.

Hacker: Persona dedicada a lograr un conocimiento profundo sobre el funcionamiento interno de un sistema, de una PC o de una red con el objeto de alterar en forma nociva su funcionamiento.

Internet: Red privada dentro de una empresa, que utiliza el mismo software y protocoles empleados en la internet global, pero que solo es de uso interno.

Lan: (Local Area Network). (Red de Area Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Log: Registro de datos lógicos, de las acciones o sucesos ocurridos en los sistemas aplicativos y operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoria.

Megabyte MB: Es bien un millón de bytes ó 1.048.576 bytes.

Messenger: Opción de mensajería instantánea disponible en Internet. Puede traer problemas en las redes y sistemas privados, por cuándo puede convertirse en una herramienta de trafico de virus y publicidad no solicitada así como una canal vulnerable para la seguridad de redes y servidores.

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de manera que puedan compartir recursos.

Seguridad: Mecanismos de control que evitan el uso no autorizado de recursos.

Servidor: Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Servidor de correo: Dispositivo especializado en la gestión del tráfico de correo electrónico. Es un servidor perteneciente a la red de Internet, por lo que tiene conexión directa y permanente a la Red Pública. Su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.

S.O: (Sistema Operativo). 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.

Virus: Programa que se duplica a si mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de Troya o gusano).

Monitoreo de Cuentas de correo: Vigilancia o seguimiento minuciosos de los mensajes de correo que recibe y envía un usuario.

Web Site: Un Web Site es equivalente a tener una oficina virtual o tienda en el Internet disponible para ser accesado y consultado por todo navegante en la red pública. Un Web Site es un instrumento avanzado

"La información contenida en el presente procedimiento es propiedad de IGHO SAS es SECRETA Y CONFIDENCIAL. Las personas que lo reciben son responsables por su seguridad y prevención del uso indebido"

y rápido de la comunicación que facilita el suministro de información de productos o entidades. Un Web Site es también considerado como un conjunto de páginas electrónicas las cuales se pueden accesar a través de internet.

Web Mail: Es una tecnología que permite acceder a una cuenta de Correo Electrónico (E-mail) a través de un navegador de internet, de esta forma podrá acceder a su casilla de correo desde cualquier computadora del mundo.

Responsable del proceso: será la persona encargada de:

- Velar por la seguridad y estabilidad de los activos informáticos de la institución.
- Gestionar procedimientos que salva guarden la información de la institución.
- Elaboraciones de planes de seguridad tipo hardware y software.
- Capacitaciones a los usuarios en temas de seguridad informática y otros.
- Coordinar y crear planes de contingencia que de sustento o solución a problemas de seguridad, mantenimientos preventivos y correctivos tipo hardware y software dentro de la institución.
- Orientar y guiar a los empleados con formas o métodos para evitar eventualidades que atenten con la seguridad informática de la institución.
- Informar sobre problemas de seguridad , tipo hardware y software a la alta gerencia de la institución

Y así se denominara de ahora en adelante dentro del documento

3. MARCO LEGAL

Listado del conjunto de normas y requisitos legales vigentes a los cuales se deben dar cumplimiento y que se relaciona con la elaboración del documento.

Norma	Tema o asunto
Decreto 1317	Tratamientos de datos personales y políticas de seguridad
ISO 27001	Estándar de seguridad de la información

4. POBLACIÓN OBJETO

Sera toda aquellas personas que tengan relación directa o indirectamente con la institución IGHO S.A.S denominada personas naturales y/o Jurídicas

5. PROCEDIMIENTO

5.1. POLÍTICAS ADOPTADAS

Considerando que IGHO SAS se encuentra en proceso de implementación del Sistema de Gestión de la Calidad, y teniendo encuentra que a través de políticas se propone Administrar, desarrollar y mantener en buen estado los mismos, garantizando el apoyo logístico para el buen desarrollo de la Gestión; se adoptan las siguientes políticas de seguridad informáticas en la empresa:

- Seguridad Organizacional
- Seguridad Física
- Seguridad Lógica
- Seguridad Legal

Dichas políticas son de obligatorio cumplimiento.

El funcionario que incumpla las políticas de seguridad informática, responderá por sus acciones o por los daños causados a la infraestructura tecnológica de la empresa, de conformidad con las leyes penales, fiscales y disciplinarias.

5.1.1. Seguridad Organizacional

Los servicios de la red institucional del instituto IGHO S.A.S son de exclusivo uso laboral y para gestiones administrativas o asistenciales, cualquier cambio en la normativa del uso de los mismos, será expresa y adecuada como política de seguridad en este documento.

Usuarios

Es la cuenta que constituye la principal vía de acceso a los sistemas de información que posee la empresa; estas cuentas aíslan al usuario del entorno, impidiendo que pueda dañar al sistema o a otros usuarios, y permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros.

Cada persona que acceda al sistema debe tener una sola cuenta de usuario. Esto permite realizar

"La información contenida en el presente procedimiento es propiedad de IGHO SAS es SECRETA Y CONFIDENCIAL. Las personas que lo reciben son responsables por su seguridad y prevención del uso indebido"

seguimiento y control, evita que interfieran las configuraciones de distintos usuarios o acceder al buzón de correo de otro usuario.

Una cuenta de usuario asigna permisos o privilegios al usuario para acceder a los sistemas de información y desarrollara actividades dentro de ellas. Los privilegios asignados delimitan las actividades que el usuario puede desarrollar sobre los sistemas de información y la red de datos.

Para la creación de cuentas nuevas:

- La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por escrito al **Responsable del proceso** y debe ser debidamente autorizada por la Dirección Administrativa.
- Cuando un usuario ingresa y hace parte de la red institucional, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad informática (PR-01GIN-01)
- No debe concederse un acceso a la red institucional a personas que no sean funcionaros de la empresa, a menos que estén debidamente autorizados por la Dirección administrativa.
- Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye a los administradores del sistema.
- A los funcionarios que cesan sus actividades se desactivarán acceso a la red institucional solicitud enviada por la Dirección Administrativa al responsable del proceso.
- Los privilegios especiales de borrar o depurar los archivos de otros usuarios, solo se otorgan a los Responsable del proceso y bajo la autorización de la dirección administrativa.
- No se otorgara cuentas a técnicos de mantenimientos externos, ni permitir su acceso remoto, a menos que la Dirección Administrativa determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).
- No se crearán cuentas anónimas o de invitado.
- Todo usuario que tenga acceso a la red y a información que procesa la institución deberá cumplir con el derecho a la confidencialidad y protección de información, puesto que esta información es de uso exclusivo para procesos administrativos y asistenciales del instituto y no le competen a nadie más fuera de él

Internet

Internet es una herramienta cuyo uso autoriza la empresa en forma extraordinaria, puesto que contiene ciertos peligros. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas. Se debe aplicar una política que procure la seguridad y realizar monitoreo constante, por lo que se debe tener en cuenta lo siguiente:

Políticas adoptadas para el uso adecuado de este importante servicio:

- El acceso a internet en horas laborales, es de uso solo laboral no personal, con el fin de no saturar el ancho de banda y así poder hace 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 de 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 IGHO SAS 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 Dirección Administrativa que se encargara de realizar las operaciones o solicitudes oportunas.
- Los empleados de IGHO SAS tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.
- Ningún empleado debe instalar ningún programa para ver videos o emisoras de televisión vía internet y de música. (Ares, Real Audio, BWV, etc).
- No debe usarse el internet para realizar llamadas internacionales (Dialpap, skipe, NET2PHONE, FREEPHONE, etc.).

"La información contenida en el presente procedimiento es propiedad de IGHO SAS es SECRETA Y CONFIDENCIAL. Las personas que lo reciben son responsables por su seguridad y prevención del uso indebido"

Correo Electrónico

El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional de la empresa.

Es de anotar que el correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley.

Las políticas de uso son:

- Utilizar el correo electrónico como una herramienta de trabajo, y no como nuestra casilla personal de mensajes a amigos y familiares, para esto está el correo personal.
- No facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas. Los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de servicios en internet.
- No participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.
- No distribuir mensajes con contenidos impropios y/o lesivos a la moral.
- No enviar grandes cadenas de chistes en forma interna.
- Si se recibe un correo de origen desconocido, consulten inmediatamente con el Responsable del proceso para recibir una asesoría. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc.).
- Cuando se contesta un correo evite poner "Contestar a todos" a no ser que estemos absolutamente seguros que el mensaje puede ser recibido por "todos" los intervinientes.
- El acceso a las cuentas personales debe ser mínimo (o ninguno) durante nuestra jornada laboral.
- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, no tendrán acceso a concer la contraseña asignada el responsable del proceso será la persona encargada de salvaguardar las claves de los correos institucionales mediante el usos de gestores de correo designado por la emressa ya sea de licencias pagas o gratuitas
- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
- Se debe eliminar permanentemente los mensajes innecesarios.
- Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.
- Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
- Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.
- Evitar usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.
- Evite enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la institución.
- El responsable de proceso determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.

Red Interna

- Todos los días en horarios designados por el responsable del proceso se habilitara las copias de seguridad a las bases de datos de los aplicativos misionales de la institución (estas copias de seguridad se realizarán en el servidor correspondiente, y con copia exacta a un medio de almacenamiento externo)
- No utilizar la red con fines propagandísticos o comerciales.
- No modificar ni manipular archivos que se encuentren en la red que no sean de su propiedad.
- No guardar en la red música, videos o demás archivos de uso personal ni material innecesario.

Políticas de uso de computadores, impresoras y periféricos.

"La información contenida en el presente procedimiento es propiedad de IGHO SAS es SECRETA Y CONFIDENCIAL. Las personas que lo reciben son responsables por su seguridad y prevención del uso indebido"

- La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general; no puede ser utilizado en funciones diferentes a las institucionales.
- Los usuarios no pueden instalar, suprimir o modificar el software origin
- altamente entregado en su computador. Es competencia del responsable del proceso la instalación de software.
- No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia del responsable del proceso, el retiro o cambio de partes.
- No se puede utilizar medios de almacenamiento traídos de sitios externos a la empresa, sin la previa revisión por parte del responsable del proceso para control de circulación de virus.
- No es permitido destapar o retirar la tapa de los equipos, por personal diferente al responsable del proceso o sin la autorización de esta.
- Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asigno inicialmente, sin previa autorización del responsable del proceso.
- 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 Dirección Administrativa 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 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 Dirección administrativa 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 Dirección Administrativa

5.1.2 Seguridad Física

La seguridad en red física está conformada por aquellos equipos y/o aparatos que permiten la consecución de la información.

5.1.3 Seguridad Lógica

La seguridad Lógica para la sociedad permite mantener la protección adecuada a través de los antivirus y programadas adecuados para tal fin.

5.1.4 Seguridad Legal

La seguridad legal en la información hace parte fundamental de los requisitos a los usuarios internos y externos.

5.2 OTRAS POLÍTICAS

- A los equipos portátiles personales no se les brindara soporte de ninguna índole: ni de hardware ni de software, porque no son responsabilidad del instituto por ende el dueño debe hacerse cargo y responsable de su computador.
- La dirección IP asignada a cada equipo debe ser conservada y no se debe cambiar sin la autorización del Responsable del proceso porque ocasionaría conflicto de IP'S y esto alteraría el flujo de la red.
- No llenar el espacio de disco del equipo con música, videos, ni información que no sea necesaria para el desarrollo de sus tareas con respecto a la entidad.
- Todo funcionario responsable de equipos informáticos deberá velar por la custodio y buen uso de los mismo debe dejarlo

"El correcto manejo de los equipos de sistemas de la empresa es responsabilidad directa de sus funcionarios".

"La información contenida en el presente procedimiento es propiedad de IGHO SAS es SECRETA Y CONFIDENCIAL. Las personas que lo reciben son responsables por su seguridad y prevención del uso indebido"

5.3 MECANISMOS DE SEGURIDAD

La seguridad en un sistema de información debe contemplar todas las posibles amenazas que se identifiquen sobre todos los elementos del sistema de información: maquinas, programas, datos, redes y electrónica de red. Entre las amenazas se encuentran las personas, tanto con carácter voluntario como involuntario, y las catástrofes, como los incendios e inundaciones.

La *Tabla 1* muestra los objetivos de seguridad y las medidas o mecanismo de seguridad que existen para garantizar su cumplimiento. Los dos mecanismos básicos de seguridad son las claves públicas y privadas, y los algoritmos de resumen de una dirección. Estos son los fundamentos para la construcción del resto de mecanismos de seguridad. Mediante la combinación de todos ellos se consigue proteger los sistemas de información mediante el cifrado o encriptación, la firma y los certificados digitales. Estos son los mecanismos técnicos de protección de la información.

Los mecanismos básicos y técnicos se complementan con los de organización de autorización y auditoria, así como con los de operación y de nivel de servicio.

Tabla 1. Objetivos y medidas de seguridad

OBJETIVO	DESCRIPCIÓN	MEDIDAS
1. Identificación (Autentificación)	Es el proceso de identificar al cliente de la aplicación o servicio. No olvidar que los clientes pueden ser tanto personas, como otros servicios, procesos y otros ordenadores.	Certificados digitales.
2. Confidencialidad	Consiste en asegurar que a la información solo accede quien está autorizado para ello.	Cifrado, encriptación.
3. Integridad	Conjunto de acciones que garantizan que la información no se ha transformado durante su procesado, transporte o almacenamiento.	Firma digital.
4. No repudio	Procedimientos para asegurar que ninguna de las partes implicadas ya identificadas (autentificadas) puede negar haber participado en una determinada transacción.	Firma digital, auditoría.
5. Autorización	Determinar a qué información puede acceder y qué tareas puede acometer, un cliente autentificado, por lo tanto identificado con certeza. Este proceso determina los privilegios asociados a un perfil de usuario.	Cuestión organizativa que debe diseñar cada organización y llevar a cabo en sus sistemas particulares.
6. Auditoría	Es la posibilidad de poder rastrear los accesos realizados a la información y las operaciones hechas sobre ella por cada usuario y las circunstancias en que las hizo.	Registros de acceso y operaciones efectuadas sobre la información.
7. Disponibilidad	Forma parte de la seguridad el poder disponer de la información cuando se necesite. Por ello se deben proteger los sistemas de forma que se mantengan en funcionamiento y se pueda acceder a la información en cualquier momento.	Operación y nivel de servicio adecuados sobre los sistemas.

5.4 ASIGNACIÓN DE PERFILES Y ROLES

Antes de implantar un sistema de información clínico se debe definir quién puede acceder a qué contenidos de la información y qué acciones se pueden llevar a cabo sobre ella. Es decir, se debe definir qué perfiles de usuario existen para el sistema. Indicando a qué información pueden acceder estos perfiles, qué operaciones o roles pueden realizar sobre esta información y en qué medida pueden ejercer estos roles.

Estos roles están en proceso de construcción e implementación para los usuarios internos y externos de la sociedad IGHO S.A.S.

"La información contenida en el presente procedimiento es propiedad de IGHO SAS es SECRETA Y CONFIDENCIAL. Las personas que lo reciben son responsables por su seguridad y prevención del uso indebido"