1. INTRODUCCIÓN

En GENÉTICA LAB, la información almacenada en sus servidores y estaciones de trabajo es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, por lo cual estamos comprometidos con el cumplimiento de las normativa de protección de datos, privacidad y seguridad de la información establecidas por el Gobierno Nacional, por ello se han definido las políticas para la seguridad de la información, las cuales contienen los lineamientos que deben cumplir todos los colaboradores, proveedores de bienes y/o servicios, socios y demás personas con alguna relación con el laboratorio, para garantizar la integridad, disponibilidad, confidencialidad y privacidad de la información.

2. OBJETIVO

Garantizar la protección de la información mediante la implementación y ejecución de las medias de seguridad que conlleven a preservar su integridad.

3. ALCANCE

Inicia desde la recolección o captación de La información y su circulación hasta la disposición final de la información.

4. DEFINICIONES

Para una adecuada interpretación de las políticas, se tendrá en cuenta las siguientes definiciones:

Activo. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administrador de Seguridad. Por la naturaleza de la responsabilidad, es el área CTIC, área que debe garantizar la seguridad física y lógica de los recursos informáticos, definir perfiles de acceso internos y externos, implementar herramientas de seguridad a nivel de sistemas operativos, redes y aplicaciones manteniendo en todo momento un adecuado ambiente de control.

Amenaza. Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas en sus activos.

Ataque. Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema informático.

Autenticación. Confirmación de la identidad que declaran los usuarios. Para ello se han establecidos diferentes métodos tales como, la autenticación en sitios web, análisis biométricos.

Confidencialidad. Protección de las comunicaciones o la información almacenada contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos

sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes, en materia de intimidad de los usuarios de las redes de comunicación.

Desastre o Contingencia. Interrupción de la capacidad de acceso a la información y/o procesamiento de la misma, a través de la tecnología necesaria para la operación normal de un negocio.

Disponibilidad. Significa que la información es accesibles, inclusive en casos de alteraciones, cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena, que afecten las operaciones de la empresa.

Impacto. Consecuencia de la materialización de una amenaza.

Integridad. Confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos, o en los casos en los que la exactitud de los datos es indispensable.

Licenciamiento. Contrato que celebran el autor o el que ostenta los derechos de distribución de un software con el usuario o comprador de un programa informático, para que lo pueda usar o modificar.

Riesgo. Es la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas para el cumplimiento de los objetivos Institucionales.

Segregación De Funciones. Herramienta de control que le permite a la gerencia mitigar el riesgo de fraude, ya que los procesos críticos deben ser realizados por más de una persona.

Usuario dueño. Es aquella persona responsable de administrar un aplicativo, aplicación o plataforma. Dentro de sus responsabilidades están las de definir perfiles de usuario, aprobar accesos a la aplicación o programa, informar al administrador de seguridad los cambios o retiros de los usuarios.

Usuario. Es la persona que tiene acceso a la información de acuerdo a su perfil.

Vulnerabilidad. Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

5. REFERENCIAS LEGALES

- Ley 23 de 1981(Ética Médica).
- Resolución 1995 de 1999 (Manejo de Historia GENÉTICALAB).
- Decreto 1011 de 2006 (Garantía de Calidad en Salud).
- Ley 1273 de 2009 (Delitos Informáticos).
- Acuerdo 007 de 1994 (Ley Nacional de Archivos).
- Acuerdo 037 de 2002 (Ley de Archivo).
- Ley estatutaria 1581 de 2012 (Protección de Datos Personales).

6. CONDICIONES GENERALES

6.1. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

6.1.1. Políticas en Torno a la Propiedad Intelectual.

- Toda información recolectada en las estaciones de trabajo, servidores, y equipos electrónicos y demás medios de almacenamiento, temporal o permanente, que se obtenga a través de desarrollos, investigaciones, estudios con recursos propios de GENÉTICALAB y la información que se obtenga de los pacientes como resultado de la atención, son propiedad del laboratorio GENÉTICALAB y éste se reserva los derechos sobre su uso, copia o licenciamiento.

- Los programas existentes, los nuevos desarrollos, modificaciones o cambios a aplicaciones o a programas y su documentación, manuales de usuario y manuales técnicos, son propiedad de GENÉTICALAB, en ningún momento pueden ser utilizados, copiados, comercializados, reproducidos o extraídos por los colaboradores, proveedores y demás personas relacionadas con GENÉTICALAB para beneficio propio o el de terceros.

- Licenciamiento: Todo el software instalado en los equipos de tecnología, que soportan los procesos de atención a los usuarios o administrativos y de apoyo, debe estar licenciado y autorizado.

- Protección de datos: Todos los datos relacionados con la atención del usuario como interconsulta, formularios, consentimientos, resultado y anexos, son custodiados y están protegidos contra accesos no autorizados. El acceso a la información del usuario es administrado de tal forma que solo accede el personal relacionado con su atención. El personal asistencial que va a consultar la información firmará la Cláusula de confidencialidad.

6.1.2. Políticas en Relación con la Seguridad de la Información. La integridad y la exactitud en la información, son las dos características más importantes en lo que a seguridad de la información se refiere, la primera es la garantía de que nadie puede acceder a la información, ni modificarla sin contar con la autorización necesaria y en lo referente a exactitud, es la certeza de la inexistencia de alteraciones, modificación o destrucción no autorizada de la información.

- **Integridad.** La información ingresada, procesada, consultada o extraída de los sistemas de información propios o adquiridos, debe ser real, completa y exacta, con el fin de apoyar los procesos de atención al paciente, garantizar la confiabilidad, exactitud de los datos y diagnósticos del paciente y los reportes financieros. Además, los desarrollos de nuevos programas deben basarse en las mejores prácticas, para garantizar que éstos cumplan los objetivos de integridad requeridos por la administración, implementando los controles necesarios.

- **Exactitud.** Todos los datos deben ser ingresados a los sistemas de información exactamente como son, sin ninguna modificación o cambio desde su origen.

- Para el mantenimiento de servidores, GENÉTICALAB tiene implementado la política de seguridad de la información y lista de chequeo de medidas de seguridad de la información, dicho protocolo garantiza la integridad de la información.

6.1.3. Políticas en Torno a la Confidencialidad y Privacidad de la Información. Para el cumplimiento de esta política se requiere que:

- Todos los colaboradores, socios, proveedores de bienes y/o servicios, entidades y demás entes o personas que requieran acceder a los medios tecnológicos o a la información para su labor, deben cumplir las normas o leyes relacionadas con la privacidad y confidencialidad de la información definida al interior de GENÉTICALAB, las emitidas por el Gobierno Nacional y las que a nivel internacional apliquen.

- El acceso a los medios tecnológicos, a las redes físicas e inalámbricas, programas, correos electrónicos, bases de datos, documentación física o electrónica, equipos de telecomunicaciones, servidores y demás recursos de tecnología, está restringido solo al personal con el rol, de acuerdo con el perfil del cargo que desempeña y la calidad de vinculación.

- Como medida de protección todos los contratos con proveedores de bienes y/o servicios contendrán la cláusula de confidencialidad y privacidad de la información, que prevenga a GENÉTICALAB ante demandas por uso inapropiado o violación de información.

- Los recursos tecnológicos (equipos, correo electrónico e internet, entre otros) los provee el laboratorio para el desarrollo de las actividades relacionadas con la labor de cada colaborador y en ningún caso deben ser usadas para el usufructo personal o para su entretenimiento. Los usuarios deben velar por la seguridad de la información, el buen uso y el cuidado de los recursos tecnológicos.

- Solo la Dirección del laboratorio está autorizada para dar información a los medios de comunicación externos.

- Para el caso exclusivo de acceso a la información del paciente (Historia clínica), se dará el manejo definido por la Resolución 1995 de 1999 o la normativa que derogue, modifique dicha Resolución.

- Toda persona, natural o jurídica a través de uno de sus colaboradores que por razón de sus actividades deban tener acceso a la información, se les asignará un usuario y una contraseña desde la Dirección, lo que permite identificar sus funciones dentro de los sistemas del Laboratorio, minimizando los riesgos de vulnerabilidad de la información, en la actualidad solo la Directora Administrativa y el Director tienen acceso a la modificación de las bases de datos mediante una clave.

- GENÉTICA LAB cuenta con una red (troncal cableada), y una red inalámbrica de internet. No está permitido conectar equipos personales como celulares, IPod, tabletas electrónicas, portátiles y demás dispositivos extraíbles.

6.1.4. Política en Torno a la Disponibilidad de la Información. Para el logro de esta política se debe garantizar:

- La información, los programas, las redes y demás recursos de tecnología que soporten la atención del paciente, están disponibles las 24 horas del día durante los 365 días al año.
- El acceso a la información debe estar clasificada teniendo en cuenta su alcance, contenido, su confidencialidad y al público al que va dirigida.
- Solo las áreas autorizadas por la Dirección, pueden entregar información a los entes externos e internos en los medios que se autoricen, es decir, no está permitido copiar, reproducir o extraer información de GENÉTICALAB en medios como CDs, USBs, discos duros externos y demás, sin la debida supervisión y autorización.
- GENÉTICALAB cuenta con un respaldo de la información (back-Up) que asegura la continuidad de las operaciones, ante la ocurrencia de eventos no previstos, incidentes de seguridad o desastres naturales**.**
- En el evento de la ocurrencia de una contingencia, GENÉTICALAB arrendará equipos (hardware) con las mismas especificaciones técnicas en que trabaja. Esto garantiza la continuidad en la operación.

6.1.5. Política en Torno a la Seguridad Física y Custodia de Activos

- El acceso a la información de las áreas de sistemas, sistemas de información, contratación y facturación, contabilidad, nómina, compras, debe estar restringido solo al personal autorizado y con el perfil apropiado.
- Los equipos e implementos tecnológicos deben estar configurados con las medidas de seguridad de acceso físico, según las mejores prácticas como protección a través de usuarios, claves, guayas y llaves.
- Los equipos deben ser utilizados solo con fines laborales, buscando en todo momento su uso apropiado, optimización del tiempo y debido cuidado.
- No está permitido utilizar medios de almacenamiento externo personales como USB, CD o discos duros para mantener o sustraer información de GENÉTICALAB**.**
- La reposición de equipos y la destrucción de documentos físicos está definida por la Dirección y el comité de historias clínicas.
- Todos los proveedores que utilicen los sistemas de información de la GENÉTICALAB y que tengan acceso a la información de los pacientes, deben firmar una cláusula de confidencialidad del manejo de la información.
- Los colaboradores deben estar capacitados en el uso apropiado de los equipos de tecnología y de los programas o aplicaciones que soportan sus labores. Además, GENÉTICALAB los capacita en lo referente a la cultura de control, de tal forma que se garantice la seguridad, privacidad y confidencialidad de la información y el buen uso de los sistemas, a través de a inducción y el plan de capacitaciones.

6.2. SANCIONES

Las Políticas para la seguridad de la información deben ser cumplidas por todas las personas que tienen relación laboral, comercial, civil y demás con GENÉTICALAB. En caso de evidenciarse incumplimiento de éstas, se procederá según el caso:

6.2.1. En el Caso de un Colaborador. Se iniciará un proceso disciplinario y se aplicará la sanción establecida en el Reglamento Interno de Trabajo, lo que estipule la Ley y/o el Código Laboral.

6.2.2. En el Caso de Proveedores de Bienes y/o Servicios. Se dará por terminada la relación comercial y/o civil.

Mauricio Camargo
Representante Legal