POLITICA DE SEGURIDAD DE LA INFORMACION Y PROTECCION DE DATOS QUILISALUD E.S.E

1. **DESCRIPCION DE LA POLITICA:** la ESE QUILISLAUD, en su función de ofrecer recursos informáticos, seguros, estables y confiables, elabora la Política de Seguridad de la información y protección de datos que compile las medidas tomadas con el fin de poder garantizar el cumplimiento de los lineamientos que le asegurarán a la entidad una protección continua tanto para los activos tangibles como para los intangibles.

   La ESE QUILISALUD, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales, de manera confidencial y con los mecanismos de seguridad necesarios para impedir que terceros no autorizados tengan acceso a la misma.

2. **ALCANCE:** La aplicación de la política de la ESE Quilisalud, acogería a todos los funcionarios, de planta y contratistas, asistenciales y administrativos que hagan uso de herramientas informáticas y/o estén conectados a la red de la institución y tengan accedo a registros clínicos.

   La Política de Seguridad que se implemente requiere un alto compromiso por parte de cada uno de los funcionarios de la institución, capacidad para detectar fallas y anomalías y el establecimiento de controles continuos para renovar y actualizar dicha política en función del ambiente dinámico, cambiante y evolutivo que nos rodea.

3. **OBJETIVO GENERAL:** Crear una cultura organizacional de buenas prácticas en el aspecto comunicativo y fortalecer la protección de los activos y la información en general de la entidad.

OBJETIVOS ESPECIFICOS

Establecer normas de cuidado de equipos, periféricos y demás dispositivos físicos.

Sensibilizar a todos los usuarios de Quilisalud ESE acerca de la necesidad de poner en práctica la protección de datos en conjunto con el plan de comunicaciones establecido.

Crear mecanismos de protección a partir de la toma de precauciones, básicas pero fundamentales a la hora de utilizar los recursos de red tales como internet o intranet.

Reglamentar y controlar el tipo de información institucional verbal o audiovisual que emitan los funcionarios y contratistas de la ESE Quilisalud.

Reglamentar y controlar la instalación de todo tipo de software, entre todos los funcionarios y contratistas de la ESE Quilisalud

Documentar las políticas de seguridad, creadas para la ESE y junto con el plan de contingencia, establecer los parámetros fundamentales de estabilidad y confiabilidad de datos del área informática de la institución.

4. Normatividad vigente

Atender todas las disposiciones de la Ley 527 de 1999. Que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

La Ley 594/00 Ley General de Archivos, en sus Artículos 19 y 21 establece: Art. 19 ". Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de su <sic> archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, para salvaguardar la información.

Acuerdo 060/2001 del Archivo General de la Nación "por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas. "

En cuanto a las Comunicaciones oficiales por correo electrónico, las entidades que dispongan de Internet y servicios de correo electrónico reglamentarán su utilización y asignarán responsabilidades de acuerdo con la cantidad de cuentas habilitadas. En todo caso, las unidades de correspondencia tendrán el control de los mismos, garantizando el seguimiento de las comunicaciones oficiales recibidas y enviadas. Para los efectos de acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales se deben atender las disposiciones de la Ley 527 de 1999 y demás normas relacionadas.

Del código penal Artículo 257. Del acceso ilegal o prestación ilegal de los servicios de telecomunicaciones. El que acceda o use el servicio de telefonía móvil celular u otro servicio de comunicaciones mediante la copia o reproducción no autorizada por la autoridad competente de señales de identificación de equipos terminales de éstos servicios, derivaciones, o uso de líneas de telefonía pública básica conmutada local, local extendida o de larga distancia no autorizadas, o preste servicios o actividades de telecomunicaciones con ánimo de lucro no autorizados, incurrirá en prisión de dos (2) a ocho (8) años y multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes. Texto resaltado declarado EXEQUIBLE por la Corte Constitucional mediante Sentencia de la Corte Constitucional 311 de 2002

5. Políticas de comunicaciones

POLITICAS DE SEGURIDAD EN LA INFORMACION DE USUARIOS DEL SISTEMA

Los usuarios son los colaboradores que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. La oficina de Sistemas de Información establece normas que buscan reducir los riesgos a la información o infraestructura informática. Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática, para ello se darán los siguientes lineamientos.

1. La información almacenada en los equipos de cómputo de Quilisalud ESE y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

2. Toda información en formato electrónico o impreso debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación. Con esto se alimenta el inventario y clasificación de los archivos de información.

3. Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

4. Los permisos a usuarios son personales e intransferibles y serán acordes a las

funciones que desempeñen y no deberán tener permisos adicionales a estos. Estos permisos se conceden por autorización del coordinador del proceso.

Esta totalmente prohibido: El intento o violación de los controles de seguridad establecidos; El uso sin autorización de los activos informáticos; El uso no autorizado o impropio de la conexión al Sistema; el uso indebido de la las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma

5. El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas a la oficina de Sistemas de Información.

6. Informar inmediatamente a la oficina de Sistemas de Información cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente.

7. Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos para saltar ítems en la historia clínica o de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas.

8. La oficina de Sistemas de Información es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son exclusivas de la misión y función de la institución.

9.Los usuarios recibirán capacitación para el manejo de las herramientas desarrolladas en la institución. La asistencia a la capacitación es obligatoria y requisito indispensable para acceder al sistema de información de lo contrario no se le asigna claves y contraseñas. Esta totalmente prohibido el uso de contraseñas o claves de otro usuario.

POLITICA DE SEGURIDAD DE SOFTWARE

1. La oficina de Sistemas de Información es la única responsable de la instalación de software informático y de telecomunicaciones.

2. Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales.

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

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

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

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

POLITICA DE SEGURIDAD DE LA RED E INTERNET

1. Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas de Información de la ESE Quilisalud.
2. Se prohíbe utilizar la red y los equipos de la ESE para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24: "Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."
3. En lo relacionado con el uso de correo electrónico, no está permitido el uso del correo

personal. Los correos institucionales deben ser para uso exclusivo de las actividades de la ESE QUILISALUD.

4. Para garantizar la seguridad de la información y el equipo informático, la oficina de Sistemas de Información establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad:

Se prohíbe:

. Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.

. Acceder remotamente a los equipos de la ESE, solo funcionarios autorizados

. Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.

. Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizada asi como de información.

. Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.

. Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables, al igual que el uso de redes sociales son o tienen que ver son el cumplimiento de las actividades del colaborador.

. El intercambio no autorizado de información de propiedad de la ESE de sus usuarios y/o sus funcionarios, con terceros.

. El acceso a cuentas de correos personales de ningún tipo desde la red de la ESE y solo se podrán utilizar las cuentas de correo electrónico suministradas por la Institución. Algunos ejemplos de los sistemas de correos electrónicos personales no autorizados son Yahoo, Hotmail, Gmail.

5. Los servicios bancarios vía web a nombre de la ESE, solamente podrán ser utilizados

por el jefe de tesorería y únicamente en el equipo que este tenga asignado. La oficina de Sistemas de Información tendrá habilitado otro equipo para esta tarea a fin de dar apoyo y soporte cuando se solicite.

6. El acceso a la red interna se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido únicamente por la oficina de Sistemas de Información.

7. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad.

POLITICAS DE SEGURIDAD DE DATOS E INFORMACIÓN

La información es en uno de los elementos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos. El objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.

1. Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado, por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva. Aplicación de la Ley 594 de 2000 Ley de Archivos. Tablas de Retención Documental.

2. El propietario de la información, con la participación de un funcionario de la oficina de Sistemas de Información son los encargados de la creación y seguimiento de las copias de seguridad realizadas a la información previamente seleccionada por el usuario.

3. Cualquier aplicación, archivo desconocido o sospechoso que aparezca en la información del usuario (ya sea en el equipo local, correo electrónico), no debe ser abierto o ejecutado sin antes contar con la asesoría de la oficina de Sistemas de Información, que se encargará de examinar y determinar si la aplicación o archivo es potencialmente

peligrosa para el equipo o la red de la entidad.

4. No está permitido extraer información por ningún medio y bajo ningún motivo de la institución sin autorización.

6. **Exclusiones :** Ninguna

ELABORO Y ADAPTO	REVISO:	APROBÓ:
Sergio Loboa FIRMA:	**Gonzalo Pérez Fernández** FIRMA	**Carlos Gabriel Quiñonez** FIRMA
CARGO: **líder de comunicaciones**	CARGO **Jefe de planeación y calidad**	CARGO **Gerente Quilisalud E.S.E**
FECHA: **septiembre 2020**	FECHA: **septiembre 2020**	FECHA: **septiembre 25020**