Sulíquido Slq S.A.S, consiente de la necesidad de implementar y mantener los controles adecuados tendientes a prevenir, detectar y gestionar los riesgos de seguridad en la información, define las siguientes directrices.

## POLÍTICA DE SEGURIDAD INFORMÁTICA

1. Sistemas y servicios generales es responsable del control e instalación de mecanismos de seguridad que garanticen la preservación de la información de la empresa.

2. Todas las plataformas deben cumplir con los siguientes requerimientos de seguridad:
   a. Control de acceso discrecional: Mecanismos obligatorios, que permitirán a los usuarios y administradores, compartir recursos y evitar la propagación de derechos de acceso inapropiados.
   b. Identificación y autenticación: El sistema debe estar en capacidad de identificar a cada individuo, además de permitir asociar al usuario con acciones auditables.
   c. Auditoria: El sistema debe estar en capacidad de proteger de modificaciones, accesos no autorizados o destrucción y de crear y mantener pistas de auditoría que puedan registrar eventos como uso de usuarios y claves, acciones de los operadores y/o administradores, acciones de seguridad y en general todas las acciones que puedan atentar contra los recursos del sistema.
   d. Integridad del sistema: Las características de hardware y software son provistas para que puedan ser usadas para validar periódicamente la correcta operación de los elementos del sistema.
   e. Pruebas de seguridad: Deben incluir la búsqueda de fallas obvias que puedan permitir la violación o aislamiento de recursos, o que pudieran permitir accesos no autorizados a los datos de autenticación o de auditoría.

3. La organización, podrá monitorear el uso de las herramientas de su propiedad, dadas a los empleados para el desempeño de sus funciones, tales como equipos de cómputo, software de oficina, correo, Internet, teléfono, celular, etc.

4. El Coordinador de Seguridad, deberá informar a los administradores de seguridad a nivel de las aplicaciones y de las plataformas, de cualquier retiro y/o movimiento de personal de las diferentes áreas, para verificar que procedan a eliminar los accesos otorgados a dichos empleados, y para resguardar la información

5. Los Directores de Área son los responsables de solicitar al encargado de sistemas y servicios generales la creación de un nuevo identificador de usuario con su perfil de acceso.

6. Los usuarios de la información son responsables de:
   a. Usar la información únicamente para los propósitos que la organización les indique.
   b. Cumplir con todos los procedimientos de control establecidos por la organización, incluida la custodia.
   c. Asegurarse que la información clasificada o sensible no vaya a ser suministrada a otros sin autorización de la organización.
   d. Asegurarse que sus claves de acceso individuales no serán suministradas o usadas por terceros.
   e. Familiarizarse con las guías de seguridad que la organización divulgue o suministre.
   f. Cada usuario es responsable de proteger su información de accesos no autorizados.

7. El impedimento de instalación de software se manejará por medeio de los mttos preiocodcos al software cada equipo

**POLÍTICA DE CONFIDENCIALIDAD DE LA INFORMACIÓN**

1. Independiente del medio en que se maneje (manual, sistemas de Información, verbal, etc.), tendrá el carácter de confidencial, toda la información operativa, administrativa, técnica, de producción y toda aquella que expresamente no sea oficializada a través de los niveles directivos de la compañía.

2. Incurrirán en sanciones de tipo administrativo y penal, los empleados que sean sorprendidos o se les compruebe uso inadecuado e Inapropiado de la información, o hayan manipulado información con el fin de confundir y ocultar situaciones que puedan afectar negativamente a la organización.

   Entre las sanciones a considerar dependiendo de la gravedad observada por los directivos de la empresa, están las siguientes:

a. Llamado de atención con copia a la hoja de vida.
b. Suspensión temporal de su cargo sin derecho a remuneración.
c. Cancelación del contrato de trabajo por justa causa
d. Denuncia penal cuando a ello haya lugar.

3. Es responsabilidad de todos los empleados velar por la seguridad de la información de la empresa, por lo que quien observe irregularidades a este respecto deberá informarlas a los niveles directivos que sean del caso.

4. Cada empleado debe ser informado individualmente de estas políticas. Adicionalmente las mismas deben ser publicadas en los medios internos de divulgación, tales como las carteleras, Intranet u otros de los que se disponga.

**POLÍTICA DE ANTIVIRUS**

- Ante la amenaza continua de los virus y los niveles de sofisticación implementados, se hace necesario apoyar la tarea tradicional de los programas antivirus, con el desarrollo de una cultura de salvaguarda de la información del activo que representa la información.
- Todo Computador que opere en la red de la empresa debe contar con el programa de antivirus establecido, no deben utilizar otras marcas de antivirus.
- Se debe verificar periódicamente el funcionamiento y actualización.
- Se debe hacer mantenimiento y actualización periódica al servidor de antivirus para contar con las últimas versiones de protección.
- El sistema de antivirus debe contar con el soporte y actualización vigente.

**PROCESO RECOMENDADO A USUARIOS PARA PREVENIR PROBLEMAS DE VIRUS:**

- Todo computador de la empresa debe tener instalado y en operación el antivirus establecido.
- Se deben contar con limitaciones para la descarga de archivos que no formen parte de la razón de su cargo, y solo se deberá habilitar, con la autorización del jefe del área, previa capacitación en los riesgos que implica la descarga de archivos.

- Nunca habrá archivos o macros adjuntas a un correo de procedencia desconocida, sospechosa o fuente no confiable. Borre los archivos adjuntos inmediatamente, luego haga un doble borrado, vaciando su papelera de reciclaje.
- Borre el spam, cadenas y cualquier correo chatarra. No realice reenvío de los mismos.
- Nunca descargue archivos de sitios desconocidos o fuentes sospechosas
- Siempre revise con el antivirus sus unidades de disco flexible, discos removibles o memorias flash ante de usarlas
- Respalde información crítica y configuración de sistemas en forma regular y almacene la información en un lugar seguro.

**POLÍTICA DE BACKUP DE LA INFORMACIÓN**

1. Los archivos de todos los usuarios (Incluidos gerentes y contratistas que tengan acceso a información de la compañía), serán direccionados a una unidad de red que tendrá las configuraciones de seguridad que permitirán el acceso privado a los documentos de cada uno de los usuarios.

2. Para asegurar que este procedimiento se esté cumpliendo se debe realizar inspecciones de sincronización de los archivos mensualmente.

3. Se realizará copia del archivo de datos de correo electrónico, la cual será verificada por el administrador de backup. En el caso de usuarios con computador portátil, se debe garantizar la copia una vez al mes.

4. Para efectos de administración y ejecución de los backup, Sistemas y Servicios Generales es el responsable de administrar las copias de seguridad.

5. Es responsabilidad de Sistemas y Servicios Generales hacer revisión mensual de los registros de control de los backup.

**POLITICA DE MANEJO DE CONTRASEÑAS SEGURAS**

Para gestionar correctamente la seguridad de las contraseñas se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave.

2. Se recomienda utilizar en una misma contraseña dígitos, letras mayúsculas, minúsculas y caracteres especiales.

3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas.

4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.

5. Las contraseñas se deben cambiar regularmente.

**ACCIONES QUE DEBEN EVITARSE EN LA GESTIÓN DE CONTRASEÑAS SEGURAS**

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios.

2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como la cedula o número de teléfono.

3. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)

4. No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

5. Evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.

6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.

7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej. no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).

8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador)

9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como *“ataque por diccionario”*.

10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.

11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o “*vuelta atrás*”.

12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.

13. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).

**POLITICA PARA EL USO DE INTERNET**

1. El uso de Internet es exclusivamente para las actividades de la empresa y para los ratos libres estipulados por Suliquido Slq S.A.S

2. A través de los equipos de monitoreo y análisis de tráfico instalados por el área de TI, se detectarán a los usuarios que hagan mal uso de los Servicios de Internet.

3. Está totalmente prohibido el ingreso a paginas de contenido pornográfico, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como

pornográficos, la utilización de los recursos para distribución o reproducción, de este tipo de material ya sea vía Web o medios magnéticos.

4. Está prohibido descargar **música** y **video**.

5. Está Prohibido participar en juegos de entretenimiento en línea.

6. Verificar que todos los archivos que se copien a su computadora no contengan virus.

7. Los usuarios utilizarán únicamente los servicios para los cuales están autorizados. No deberán usar la cuenta de otra persona, ni intentar apoderarse de claves de acceso de otros, así como no deberá intentar acceder ni modificar archivos que no son de su propiedad, y mucho menos, los pertenecientes a la empresa.

8. Se debe respetar la privacidad de otros usuarios. Los archivos, discos, cintas e información, son privados; el Usuario no debe intentar leer, copiar o cambiar los archivos de otro usuario, a menos que haya sido autorizado por éste.

9. Si no está navegando por el Web, cierre todas las ventanas abiertas de su explorador

10. Cualquier archivo que se reciba por Internet debe revisarse para asegurar que no contenga virus, ya que existen algunos que pueden destruir toda la información del disco duro del equipo. Antes de abrir cualquier archivo recibido por Internet, el usuario debe asegurarse de que sea un archivo confiable.

11. Se prohíbe la instalación de programas y la modificación de los programas, paquetes y configuraciones ya instalados en las estaciones o red.

12. El Usuario no debe interferir en los procesos computacionales de la empresa mediante acciones deliberadas que disminuyan el desempeño o la capacidad de los equipos instalados. Así mismo y bajo ningún pretexto debe intentar burlar los esquemas de seguridad de la Empresa.

13. No deje prendido su computador, sin hacer uso de ella, por largos periodos de tiempo, si va a dejar de usarlo permanentemente, cierre las aplicaciones (navegadores o clientes de correo) que esté usando.

14. Cambie con frecuencia sus claves de acceso a servicios y no se las comunique a nadie, (de preferencia, que sus contraseñas incluyan letras, mayúsculas y minúsculas, números y caracteres especiales, que sean de una longitud mínima de 8 caracteres. Y que no formen palabras o información conocidas por ejemplo, la fecha de nacimiento).

15. No instale software libre (freeware o shareware) a menos que esté seguro que su uso no alterará el correcto funcionamiento de su computadora.

16. No desactive el antivirus de su equipo.

**SANCIONES**

I. Si se incurre en alguna de las acciones anteriores, se tomarán las medidas disciplinarias, de acuerdo con el Reglamento Interno de Trabajo.