

CONTENIDO

1. INTRODUCCION.....

2.OBJETIVOS DE LA POLITICA

3.POLÍTICAS GENERALES

4. ALCANCE

5. USO DE INTERNET

a. Identificación única por usuario

b. Uso Adecuado de Internet.....

c. Mal Uso del Internet.....

6. USO DEL SISTEMA DE CORREO ELECTRÓNICO

a. Propiedad del Sistema y la Información

b. Usos Autorizados.....

c. Identidad del Usuario en los Mensajes

d. Privacidad

e. Mal Uso del Correo Electrónico.....

6. USO DEL CHAT CORPORATIVO

a. Propiedad del Sistema y la Información

b. Usos Autorizados.....

c. Privacidad

d. Mal Uso del Chat Corporativo.....

7. DEBERES PARA EL BUEN USO DE LAS HERRAMIENTAS
ELECTRÓNICAS

2

2

2

2

2

3

3

3

4

4

4

4

4

5

5

5

5

6

6

6

6

7

1. INTRODUCCION

La Superintendencia de Vigilancia y Seguridad Privada se encuentra implementando una herramienta de colaboración electrónica en modalidad de SaaS (Software As A Service /Nube) que le permita a la Entidad utilizar los servicios de cuenta de correo electrónico individual, calendario individual que permita crear y compartir eventos con otros usuarios, suite de ofimática (procesadores de texto, hoja de cálculo y presentaciones) en línea, servicio de mensajería instantánea (chat corporativo) y acceso por medio de dispositivos móviles a los servicios anteriores. Lo que hace necesario crear una política que minimice el riesgo frente a los recursos de información comprometidos, violando políticas, estatutos o la confianza otorgada a los miembros de la Entidad.

Este documento pretende completar y no sustituye las normas de cumplimiento, documentos normativos, circulares, o memorandos aprobados por la Superintendencia de Vigilancia y Seguridad Privada.

2.OBJETIVOS DE LA POLITICA

Establecer los alineamientos básicos y de uso del internet, correo electrónico y chat corporativo, mejorando el control y seguridad de la información. Mejorar las comunicaciones e incorporar en la cultura organizacional el uso de herramientas electrónicas colaborativas. Alinearse con la política de “cero papel” difundida y apoyada por el Gobierno Nacional.

3.POLÍTICAS GENERALES

- Toda la información enviada y recibida, contenida, procesada o generada en dichas herramientas de la Entidad son propiedad de la Superintendencia de Vigilancia y Seguridad Privada.
- Todos los funcionarios, contratistas y terceros de la Supervigilancia que tenga acceso al Internet, correo electrónico (E-mail) o chat corporativo, utilizando la infraestructura de la Entidad, tienen la obligación de mantenerse informados acerca de cualquier norma y reglamentación que aplique para su correcto uso.

4. ALCANCE

- La política aplica a todos los funcionarios, contratistas y terceros que usen estas herramientas de la Superintendencia de Vigilancia y Seguridad Privada ya sea que accedan a ellas en forma local desde la Entidad o lo hagan a través Internet por fuera de la Supervigilancia. En lo que sigue, la palabra “usuario” se referirá a cualquiera de estas personas.

5. USO DE INTERNET

Los privilegios de uso de Internet estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

Las solicitudes de creación de nuevo usuario y los cambios de privilegios de acceso se presentarán a través del Sistema de Soporte Técnico (Ticket) por el jefe del área a la que pertenezca el usuario.

Se podrán otorgar derechos de acceso a personas ajenas a la Supervigilancia (contratista), siempre y cuando la solicitud haya sido presentada por el jefe del

área en el que prestará sus servicios o supervisor del contrato; igualmente, es responsabilidad del jefe del área o supervisor del contrato solicitar el retiro de dichos permisos cuando lo considere necesario y/o haya terminado la prestación de sus servicios a la Entidad.

a. Identificación única por usuario

Cada usuario contará con un código de usuario para su equipo (PC o Portátil) y una contraseña única. Sin importar la circunstancia, está prohibido compartir o revelar la contraseña a otros usuarios. La autenticación en los medios electrónicos se hace a través de la contraseña intransferible, lo que significa que es responsabilidad de cada usuario la información y mensajes que fluyan a través de ellos. Para prevenir el uso indebido de contraseñas, el usuario deberá cambiar la suya con la frecuencia que está configurada en las políticas del servidor el cual indicará su vencimiento de esta.

Se prohíbe el control de acceso a archivos, aplicaciones, bases de datos, computadores ó redes por medio de contraseñas compartidas (**no se crearán contraseñas aplicables a grupos de usuarios**). Es obligación de cada Delegado, Jefe, Coordinador o Supervisor reportar de inmediato a la Oficina de Informática y Sistemas los cambios de personal que puedan afectar el uso del sistema, como traslados, retiros, suspensiones, vacaciones o permisos.

b. Uso Adecuado de Internet

Debe entenderse que Internet es una herramienta estrictamente de trabajo y no con otros fines ajenos a las funciones del usuario.

Los accesos a la red (Internet) serán sólo de interés laboral y no personal.

c. Mal Uso del Internet

De ninguna manera se podrá acceder a páginas web de entretenimiento, pornografía o fuera del contexto laboral.

El usuario no deberá bajar (ó copiar) archivos de la red sin autorización de la Oficina de Informática y Sistemas.

No debe usarse el Internet para acceder a redes sociales (Facebook, Twitter, etc.).

El usuario no debe bajar ningún programa ni ejecutar (software), sin la debida autorización de la Oficina de Informática y Sistemas, tales como: Shareware, software de evaluación, programas de entretenimiento, etc., ya que estos no poseen licencia para su uso en la Supervigilancia y pueden ocasionar daños a los sistemas e información alojados en los equipos.

El usuario no debe instalar ningún programa para entretenimiento como, por ejemplo: música (MP3, RA, WAV); emisoras de radio vía Internet. (Winamp, REAL AUDIO, MUSIC MATCH, Oozic PLAYER); para ver vídeos o emisoras de televisión vía Internet. (REAL AUDIO, BWV, etc.).

No debe usarse el Internet para realizar llamadas locales, nacionales o internacionales (Dialpad, NET2PHONE, FREEPHONE, etc.)

No se puede realizar ningún tipo de compras a través del internet institucional.

Todos los funcionarios, contratistas y terceros que tenga acceso a la Internet que realicen actividades no autorizadas, podrán estar sujeto a investigaciones disciplinarias, de acuerdo al rol que cumple en el entorno de la Supervigilancia.

Al ser encontrado algún funcionario, contratista o tercero dándole mal uso al Internet, la Oficina de Informática y Sistemas o quien lo detecte procederá a comunicarle al Delegado, Jefe, Coordinador o Supervisor sobre el mal uso que se le está dando a Internet en su área.

6. USO DEL SISTEMA DE CORREO ELECTRÓNICO

El uso del correo electrónico o E-mail como comúnmente se le conoce constituye una poderosa herramienta de trabajo, que permite la transferencia de información, no sólo dentro de la Entidad, sino externamente, en forma eficiente, ágil y económica; y cualquier uso indebido del mismo puede afectar severamente la imagen y la reputación de la Supervigilancia.

Es por estas razones que la Superintendencia de Vigilancia y Seguridad Privada, entiende que el correo electrónico constituye un recurso de la Entidad, y por lo tanto debe regirse por todas las políticas y procedimientos que aplican a cualquier recurso propiedad de la Supervigilancia.

a. Propiedad del Sistema y la Información

Como una forma de aumentar la productividad, la Supervigilancia incentiva el uso de medios electrónicos como Internet, correo electrónico y chat corporativo, como una forma de mejorar la comunicación institucional.

Los sistemas de comunicación y todos los mensajes generados o manejados por el sistema de comunicación electrónica de la Supervigilancia, incluyendo las copias de respaldo, se consideran propiedad de la Supervigilancia.

El correo electrónico pertenece a la Superintendencia de Vigilancia y Seguridad Privada, es parte de su sistema de información, su uso es solamente para propósitos laborales.

La Oficina de Informática y Sistemas de la Supervigilancia es la responsable de proveer las facilidades para el acceso al correo electrónico a cualquier usuario autorizado, así como su administración.

b. Usos Autorizados

En general, el uso del sistema de correo electrónico está restringido a asuntos oficiales, su empleo para asuntos personales no está autorizado.

Está prohibido utilizar el sistema de correo electrónico para el desarrollo de actividades políticas, comerciales o de entretenimiento o para la transmisión de mensajes vulgares u obscenos.

Todos los usuarios que posean acceso autorizado al correo electrónico, deberá mantener un adecuado, ético y responsable uso de éste recurso, cuidando no dañar la imagen y reputación de la Supervigilancia, ni de ninguno de sus usuarios.

c. Identidad del Usuario en los Mensajes

En todos los mensajes deberá aparecer de acuerdo con el manual de comunicaciones de la Superintendencia de Vigilancia y Seguridad Privada el

nombre del usuario, su cargo que desempeña, el nombre de la Superintendencia de Vigilancia y Seguridad Privada, la dirección y el número del PBX.

d. Privacidad

Toda información almacenada, desarrollada o transmitida por correo electrónico, utilizando los recursos e infraestructura de la Entidad, es propiedad de la Superintendencia de Vigilancia y Seguridad Privada.

Ningún usuario de una cuenta de correo electrónico de la Supervigilancia tiene derecho a la confidencialidad en relación con cualquier información o mensaje creado, recibido o enviado a través del correo electrónico institucional. Su uso estará sujeto a auditorías internas sin previo aviso. Se entiende que la Supervigilancia a través de quien el Superintendente o Secretario General determinen puede leer en cualquier momento lo que se escriba a través del sistema.

La Oficina de Control Interno puede auditar sin previo aviso el uso del correo electrónico para cerciorarse que el recurso está siendo utilizado de manera eficiente y adecuada para propósitos y gestiones relacionadas con la Superintendencia de Vigilancia y Seguridad Privada.

e. Mal Uso del Correo Electrónico

Ninguno de los usuarios deberá utilizar el correo electrónico institucional para enviar información que no sea propia del ejercicio de sus funciones y que esté enmarcada dentro de la ejecución de las mismas, como tampoco para divulgar información de carácter privado o confidencial a cargo de la Entidad, ni para dar a conocer decisiones administrativas que no se encuentren en firme y debidamente ejecutoriadas.

Está terminantemente prohibido el uso del correo electrónico institucional para realizar cualquier otra actividad o transacciones para el desarrollo de actividades de envío de comunicaciones con la intención de difamar u ofender; así como están prohibidos mensajes, comentarios, caricaturas o chistes de carácter sexual o racial que puedan ser considerados como hostigamiento o falta de respeto hacia otras personas. También se consideran violaciones a esta política los siguientes casos: comunicaciones tipo cadenas, pornografía, chistes, venta de productos o servicios, promoción a actividades que no son patrocinadas por la Entidad, y mensajes de índole político o religioso, entre otros.

Todos los funcionarios, contratistas y terceros que tenga una cuenta de correo electrónico de la Supervigilancia que realicen actividades no autorizadas, podrán estar sujeto a investigaciones disciplinarias, de acuerdo al rol que cumple en el entorno de la Entidad.

Al ser encontrado algún funcionario, contratista o tercero dándole mal uso al correo electrónico institucional, la Oficina de Informática y Sistemas o quien lo detecte procederá a comunicarle al Delegado, Jefe, Coordinador o Supervisor sobre el mal uso que se le está dando al correo electrónico en su área.

6. USO DEL CHAT CORPORATIVO

El uso del Chat Corporativo hace parte de la herramienta de colaboración electrónica Google Apps, constituyéndose en otro instrumento de trabajo, que permite la mensajería instantánea, no sólo dentro de la Entidad, sino externamente, en forma eficiente, ágil y económica; y cualquier uso indebido del mismo puede afectar la operación y buena marcha de las funciones de cada persona y por ende de la Supervigilancia.

Es por estas razones que la Superintendencia de Vigilancia y Seguridad Privada, entiende que el Chat Corporativo constituye un recurso de la Entidad, y por lo tanto debe regirse por todas las políticas y procedimientos que aplican a cualquier recurso propiedad de la Supervigilancia.

a. Propiedad del Sistema y la Información

Como una forma de aumentar la productividad, la Supervigilancia incentiva el uso de medios electrónicos como Internet, correo electrónico y chat corporativo, como una forma de mejorar la comunicación institucional.

Los sistemas de comunicación y todos los mensajes generados o manejados por el sistema de comunicación electrónica de la Supervigilancia, incluyendo las copias de respaldo, se consideran propiedad de la Supervigilancia.

El Chat Corporativo pertenece a la Superintendencia de Vigilancia y Seguridad Privada, es parte de su sistema de información, su uso es solamente para propósitos laborales.

b. Usos Autorizados

En general, el uso del sistema de Chat Corporativo está restringido a asuntos oficiales o laborales, su empleo para asuntos personales no está autorizado.

Está prohibido utilizar el sistema de Chat Corporativo para el desarrollo de actividades políticas, comerciales o de entretenimiento o para el envío de mensajes vulgares u obscenos.

Todos los usuarios que posean acceso autorizado al Chat Corporativo, deberá mantener un adecuado, ético y responsable uso de éste recurso, cuidando no dañar la imagen y reputación de la Supervigilancia, ni de ninguno de sus usuarios.

Debe entenderse que el Chat Corporativo es una herramienta estrictamente de trabajo y no con otros fines ajenos a las funciones del usuario.

c. Privacidad

Toda información almacenada, desarrollada o transmitida por el Chat Corporativo, utilizando los recursos e infraestructura de la Entidad, es propiedad de la Superintendencia de Vigilancia y Seguridad Privada.

Ningún usuario del Chat Corporativo de la Supervigilancia tiene derecho a la confidencialidad con relación a cualquier información o mensaje creado, recibido o enviado a través de este medio. Su uso estará sujeto a auditorías internas sin previo aviso. Se entiende que la Supervigilancia a través de quien el Superintendente o Secretario General determinen puede leer en cualquier momento lo que se escriba a través del sistema.

La Oficina de Control Interno puede auditar sin previo aviso el uso del Chat Corporativo para cerciorarse que el recurso está siendo utilizado de manera eficiente y adecuada para propósitos y gestiones relacionadas con la Superintendencia de Vigilancia y Seguridad Privada.

d. Mal Uso del Chat Corporativo

Ninguno de los usuarios podrá utilizar el Chat Corporativos para enviar información que no sea propia del ejercicio de sus funciones y que esté enmarcada dentro de la ejecución de las mismas, como tampoco para divulgar

información de carácter privado o confidencial a cargo de la Entidad, ni para dar a conocer decisiones administrativas que no se encuentren en firme y debidamente ejecutoriadas.

Está terminantemente prohibido el uso del Chat Corporativos para realizar cualquier otra actividad o transacciones para el desarrollo de actividades de envío de comunicaciones con la intención de difamar u ofender; así como están prohibidos mensajes, comentarios, caricaturas o chistes de carácter sexual o racial que puedan ser considerados como hostigamiento o falta de respeto hacia otras personas. También se consideran violaciones a esta política los siguientes casos: mensajes tipo cadenas, pornografía, chistes, venta de productos o servicios, promoción a actividades que no son patrocinadas por la Entidad, y mensajes de índole político o religioso, entre otros.

Todos los funcionarios, contratistas y terceros que tenga Chat Corporativo de la Supervigilancia que realicen con él actividades no autorizadas, podrán estar sujeto a acciones disciplinarias, de acuerdo al rol que cumple en el entorno de la Entidad.

Al ser encontrado algún funcionario, contratista o tercero dándole mal uso al Chat Corporativo, la Oficina de Informática y Sistemas o quien lo detecte procederá a comunicarle al Delegado, Jefe, Coordinador o Supervisor sobre el mal uso que se le está dando al chat institucional en su área.

7. DEBERES PARA EL BUEN USO DE LAS HERRAMIENTAS ELECTRÓNICAS

Teniendo cuenta El Código Disciplinario Único (Ley 734 de 2002), establece dentro de los deberes y prohibiciones para los servidores públicos, los siguientes:

Art. 34. Son deberes de todo servidor público: ...

"4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función..."

"11. Dedicar la totalidad del tiempo reglamentario de trabajo al desempeño de las funciones encomendadas, salvo las excepciones legales".

"21. Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados".

"22. Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización".

Art. 35. A todo servidor público le está prohibido: ...

"9. Ejecutar en el lugar de trabajo actos que atenten contra la moral o las buenas costumbres".