1. RESUMEN

La organización busca publicar una Política de Uso Aceptable para los Sistemas de Información, Internet y Correo Electrónico, no con el objetivo de imponer restricciones contrarias a los valores de apertura, confianza e integridad que promueve. Por el contrario, se compromete a proteger a sus empleados, socios y la empresa frente a acciones ilegales o perjudiciales, ya sean intencionales o no. Además, los sistemas de información, como los servidores FTP con carpetas críticas identificadas, así como el uso de Internet y correo electrónico, propiedad de la organización, deberán destinarse exclusivamente a fines comerciales alineados con los intereses de la compañía y sus clientes.

2. OBJETIVO

El objetivo de este documento es establecer y especificar las directrices para el uso apropiado de los Sistemas de Información, Internet y Correo Electrónico dentro de la organización, con el propósito de resguardar tanto a los usuarios como a la organización frente a posibles riesgos que comprometan los sistemas y la información almacenada en ellos. Esta política es de cumplimiento obligatorio para todo el personal de la organización, así como para cualquier persona que acceda a estos recursos, sin excepción alguna. En consecuencia, todo usuario interno o externo que utilice estos activos de información deberá acatar lo establecido en la misma.

3. ALCANCE

Esta política abarca el uso de los Sistemas de Información, Internet y Correo Electrónico dentro de la organización. Todo el personal, incluidos empleados, contratistas, consultores, trabajadores temporales y otros colaboradores de la organización y sus subsidiarias, tiene la

responsabilidad de utilizar estos recursos de manera adecuada y con criterio. Su uso debe alinearse con las políticas y normativas internas de la organización, así como con las leyes y regulaciones locales aplicables.

4. POLÍTICA

La política de uso aceptable busca optimizar los procesos y elevar la calidad en la prestación de servicios a los usuarios. La mejora en el funcionamiento de los Sistemas de Información requiere regular su uso adecuado, gestionar sus componentes y equipos, e implementar las medidas necesarias para proteger la confidencialidad de la información. Para alcanzar estos objetivos, es esencial definir políticas que aseguren un uso eficiente y seguro de los Sistemas de Información y sus herramientas asociadas. Este documento establece las normas fundamentales que deben guiar el comportamiento de los empleados para garantizar la correcta utilización de estos recursos. Las normas serán revisadas, actualizadas y publicadas de forma periódica, siendo responsabilidad de los usuarios mantenerse al día con su contenido.

4.1 NORMAS GENERALES APLICABLES AL USO DE LOS SISTEMAS DE INFORMACIÓN

4.1.1 NORMA N°1

- Los sistemas de información de la organización, incluidos el Sistema de Gestión de Programas/Aplicaciones (como el Sistema de Gestión de Tickets) y los archivos electrónicos (carpetas relacionadas con Proyectos, Licitaciones, áreas Administrativas y Contabilidad), deben utilizarse exclusivamente para actividades vinculadas al cumplimiento de las responsabilidades asignadas a los usuarios de la organización. Esta restricción también se extiende a la información almacenada

en los equipos de cómputo de los usuarios, así como a aquella generada o transmitida a través de los sistemas de información de la entidad.

4.1.2 NORMA N°2

- El uso de los Sistemas de Información y sus herramientas asociadas, como el correo electrónico y la conexión a Internet, estará limitado exclusivamente al personal autorizado por la organización.
- Cada área será responsable de definir las tareas que requieran acceso a estas herramientas, cuyo uso debe estar orientado únicamente a fines profesionales con el propósito de optimizar las operaciones de la organización.
- El uso de estos recursos para fines personales está estrictamente prohibido. Toda la información generada, transmitida o almacenada en los Sistemas de Información de la organización es propiedad de esta.
- Las disposiciones legales aplicables a documentos privados son también de aplicación para los activos de información identificados, como Carpetas de Proyectos, Carpetas de Licitaciones y Carpetas de áreas Administrativas y Contabilidad. La divulgación no autorizada de dicha información está terminantemente prohibida.
- Cualquier acción de alteración, destrucción o distribución malintencionada o fraudulenta de documentos electrónicos pertenecientes a la organización puede afectar gravemente su desempeño y constituye una infracción grave. Ante tales situaciones, la organización adoptará las medidas disciplinarias correspondientes y se reserva el derecho de emprender acciones legales cuando sea necesario.

4.1.3 NORMA N°3

- La modificación de archivos almacenados en la Carpeta de Proyectos, Carpeta de Licitaciones, Carpetas de áreas Administrativas y Contabilidad, o cualquier otra que contenga información sensible de la organización, está estrictamente prohibida sin la autorización previa del Gerente, el Jefe del área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI). Esta medida tiene como objetivo garantizar la legalidad y la seguridad en el manejo y tratamiento de la información.

4.1.4 NORMA N°4

- Los usuarios de los sistemas de información tienen la responsabilidad de respetar los derechos de propiedad intelectual de los creadores de obras, programas, aplicaciones, archivos y cualquier otro material gestionado o accedido mediante dichos sistemas.

4.1.5 NORMA N°5

- El uso del cliente del Sistema de Gestión de Ticket, así como de los programas y recursos empleados en la organización, debe contar con la aprobación de las áreas correspondientes en las que cada empleado desempeña sus funciones.
- La instalación del cliente del Sistema de Gestión de Ticket será realizada exclusivamente por personal autorizado. Además, los programas y aplicaciones proporcionados por la organización no podrán reproducirse sin previa autorización ni emplearse para propósitos ajenos a las responsabilidades y tareas asignadas por la entidad.

4.1.6 NORMA N°6

- La organización se encargará de definir las normativas para la asignación de las cuentas de acceso, lo que incluirá la implementación de medidas de seguridad correspondientes, como contraseñas, claves secretas, controles de acceso a los servidores y sistemas, así como auditorías para garantizar el uso adecuado, la integridad y la seguridad de los datos y comunicaciones enviadas.

4.1.7 NORMA N°7

- Los usuarios de los sistemas deberán adherirse a todas las normas de uso y las relacionadas con la seguridad de la información establecidas por la organización.

4.1.8 NORMA N°8

- Cada usuario será responsable de manera individual del manejo adecuado de las claves de acceso o contraseñas que se le asignen.

4.1.9 NORMA N°9

- La asignación de claves de acceso no impedirá que el uso de los Sistemas de Información sea auditado por el personal autorizado, ya sea interno o externo, con el fin de asegurar el uso adecuado de los recursos.

4.1.10 NORMA N°10

- El acceso no autorizado a información o a una cuenta ajena, logrado mediante la modificación de privilegios de acceso o la interceptación de información de cualquier forma, está prohibido y será sujeto a las medidas disciplinarias correspondientes.

4.1.11 NORMA N°11

- El responsable de la custodia de la información, un rol asignado en la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, será el

encargado de velar por la protección de la información almacenada en los Sistemas de Información.

- El Comité de Gestión de Seguridad de la Información (CGSI) establecerá las pautas necesarias para prevenir accesos no autorizados y definir las políticas correspondientes para asegurar su integridad.

4.1.12 NORMA N°12

- Las normas establecidas deben considerarse como un complemento a las leyes nacionales aplicables en este ámbito. Además, el incumplimiento de estas normas puede resultar en la revocación de cualquier privilegio de acceso a los Sistemas de Información, y se notificará al responsable del área correspondiente, al Oficial de Seguridad de la Información y al Comité de Gestión de Seguridad de la Información (CGSI).

4.1.13 NORMA N°13

- Cualquier incumplimiento de las normas establecidas en esta Política de Uso Aceptable deberá ser comunicado al área de Recursos Humanos para su inclusión en el expediente del trabajador y para su conocimiento. Esto conllevará las acciones disciplinarias pertinentes.

4.1.14 NORMA N°14

- Los usuarios de la organización deberán emplear el Sistema de Gestión de Tickets para reportar incidencias informáticas y hacer las solicitudes pertinentes al personal responsable de Seguridad de la Información.

4.2 NORMAS APLICABLES AL USO DE INTERNET Y DEL CORREO ELECTRÓNICO

4.2.1 NORMA N°1

- Los sistemas de comunicación y el acceso a Internet de la organización deben ser utilizados exclusivamente para fines laborales, conforme a las políticas que regulan el comportamiento del personal, y no para actividades personales.

4.2.2 NORMA N°2

- Las acciones realizadas a través de Internet pueden generar responsabilidad para la organización. Por lo tanto, la organización se reserva el derecho de intervenir y auditar los accesos de los usuarios a la red y a Internet, así como el contenido al que se accede.

4.2.3 NORMA N°3

- La organización establecerá las pautas para la asignación de cuentas de correo electrónico, las medidas de seguridad aplicables, claves de acceso y contraseñas, controles de acceso a los servidores, y el proceso de auditoría del sistema y las comunicaciones enviadas.

4.2.4 NORMA N°4

- El sistema de correo electrónico y el dominio de la organización son propiedad de la misma. En consecuencia, la organización puede intervenir, auditar e investigar el uso adecuado del sistema. Las cuentas estarán sujetas a auditorías y revisiones sin previo aviso, realizadas por personal autorizado de la organización, encargado de la Seguridad de los Sistemas de Información. Los usuarios internos deben cumplir con los requisitos establecidos por la organización.

4.2.5 NORMA N°5

- La organización implementará normativas sobre el envío de documentos por correo electrónico que contengan información confidencial o sensible de la organización o relacionados con asuntos internos no divulgables. Si es necesario enviar dicha información, esta debe ser cifrada. En caso de sospecha de interceptación o divulgación, se deberá informar inmediatamente al Oficial de Seguridad de la Información para tomar las acciones correspondientes.

4.2.6 NORMA N°6

- Está expresamente prohibido acceder, ver o descargar material relacionado con pornografía o sitios maliciosos. Toda comunicación electrónica que sea amenazante, discriminatoria (por raza, credo, color de piel, edad, sexo, condiciones físicas o mentales, orientación sexual, etc.), difamatoria u ofensiva está prohibida. Asimismo, está prohibida la alteración o destrucción de comunicaciones electrónicas con la intención de causar daño a la organización o a sus miembros.

4.2.7 NORMA N°7

- Los usuarios que accedan al Correo Electrónico mediante acceso OWA (vía Internet) deben utilizar un doble factor de autenticación. Este sistema, integrado con el Directorio Activo (AD), enviará un mensaje de texto (SMS) al celular proporcionado por la organización. El acceso vía OWA está limitado a una lista de usuarios designados por la organización, la cual se ampliará conforme se justifiquen nuevos accesos y sean aprobados por el Jefe inmediato y el Comité de Gestión de Seguridad de la Información (CGSI).

5. CUMPLIMIENTO DE POLÍTICA

5.1 MEDICIÓN DEL CUMPLIMIENTO

La organización realizará un seguimiento y verificación del cumplimiento de esta política mediante una variedad de métodos, incluyendo:

- Visitas periódicas
- Monitoreo de video
- Informes generados por herramientas comerciales
- Auditorías internas y externas
- Inspecciones

Los resultados de estas actividades serán comunicados al propietario de la política y al gerente de la unidad de negocio correspondiente, con el fin de garantizar el cumplimiento y la mejora continua de la política.

5.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

5.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

6. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: