CONTENIDO

1. OBJETIVO

El propósito de este documento es definir la Política Organizacional con respecto al uso y prohibiciones de los sistemas de información en **ACESCO**.

"Todo empleado y tercero autorizado por la empresa, deberá seguir las normas, políticas y buenas prácticas establecidas en la presente Política".

2. ALCANCE

Esta política se aplicará a todos los empleados, proveedores, contratistas, consultores, aprendices, trabajadores en misión y a cualquier otra persona que tenga acceso a los sistemas de información de la Organización. También se aplica esta política a todos los equipos y sistemas informáticos -*servidores, computadores personales, estaciones de trabajo, elementos de infraestructura tecnológica, dispositivos móviles, portátiles, asistentes digitales personales, bases de datos, sistemas de información*- que apoyan los procesos de producción o administrativos que se encuentren bajo responsabilidad operacional de **ACESCO**, así como también a aquellos dispositivos de uso personal que ingresen a la misma.

3. GLOSARIO

Para los propósitos de esta política se aplicarán las siguientes definiciones:

ACESCO: ACESCO COLOMBIA S.A.S.

COMUNICACIONES ELECTRÓNICAS: incluye todo uso de los sistemas de información para comunicar, publicar material y contenido por medio de servicios como correo electrónico, chats, foros de discusión, paginas HTML o -herramientas similares.

MATERIAL NO PERMITIDO: incluye la transmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable. Se incluye sin limitación, correos electrónicos de tipo cadena, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la

propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio, ilegal bajo las leyes nacionales, racismo, violencia y demás contenidos que contravengan los principios y valores socialmente aceptados.

RED DE DATOS: es el conjunto de recursos de conectividad computacionales que permite la comunicación de datos e información a través de toda la Organización incluyendo el correo interno, externo e Internet.

REDES: incluye cualquier sistema de cableado o inalámbrico; equipos físicos como enrutadores, switches, además de sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.

SISTEMAS DE INFORMACIÓN: incluye cualquier sistema o aplicación de software que sea administrado por la Organización y de los cuales ella es responsable, además, aplicaciones de servidores y escritorio, sistemas operativos y aplicaciones de Internet.

USUARIO(S): incluye toda persona no necesariamente vinculada con la empresa, a quien ésta proporcione los medios y niveles de automatización y acceso necesarios para hacer uso de los servicios o sistemas de información de ésta.

4. DOCUMENTOS DE REFERENCIA

- M-691 Código de Ética.

5. POLITICA

ACESCO provee el acceso a todo el personal a fuentes de información nacional e internacional y promueve un ambiente digital que fomente la difusión del conocimiento, el proceso de creación y el trabajo colaborativo, en el marco del Propósito Superior de la Organización.

- Los usuarios deben hacer uso responsable y ético. Cada usuario es responsable por la integridad de estos recursos y tiene el deber de respetar los derechos de los otros usuarios, la integridad de las instalaciones físicas y sus métodos de control, además de respetar toda licencia pertinente y acuerdo contractual que esté relacionado con los sistemas de información

de la Organización.

- Los usuarios tienen la responsabilidad de informar a su jefe inmediato, y al responsable de Informática o a quien haga sus veces, de los incidentes relacionados con el uso indebido de los sistemas de información.
- **ACESCO** puede restringir o prohibir el uso de sus sistemas de información a cualquier usuario en caso de que se demuestre alguna violación de estas políticas o de alguna ley.
- **ACESCO** no asume responsabilidad alguna por el empleo de "material no permitido" en los contenidos de los correos electrónicos, así como del uso ilegal y mal intencionado del mismo por parte de sus usuarios.
- Los miembros de la Unidad de Informática con el rol específico asignado, están en la obligación de monitorear constantemente los sistemas de información de **ACESCO** a través de las herramientas informáticas disponibles o a través de auditorías externas para responder a cualquier acción que atente contra la integridad, disponibilidad, seguridad y desempeño correcto de los mismos mediante la negación, restricción de acceso a usuarios o sistemas, aislamiento y desconexión de equipos o servicios.
- La Unidad de Informática cuenta con procedimiento para el respaldo y la restauración de los sistemas de información con el objetivo de garantizar la continuidad del negocio frente a una falla y/o desastre.
- La Unidad de Informática garantizará que las versiones de los sistemas operativos usados en la empresa estén actualizados a las últimas versiones con él fin de evitar que alguna vulnerabilidad detectada, pueda ser aprovechada por un virus o atacante.
- La Unidad de Informática velará que la definición de virus del software antivirus siempre este actualizados y tomará las medidas correspondientes cuando se detecte una amenaza de virus categorizada como "Zero Day".
- La Unidad de Informática es la única dependencia autorizada para avalar la contratación de cualquier servicio tecnológico requerido, incluyendo, pero sin limitar, internet, servicios en nube, servidores, equipos de cómputo, Licencias, telefonía, impresión y otros servicios externos.
- La Unidad de Informática brindará soporte y mantenimiento sobre recursos y servicios informáticos (Software, hardware, equipos,

almacenamiento y hosting, entre otros) que estén dentro del gobierno de soporte y mantenimiento de TI.

Todos los usuarios deberán actuar de acuerdo con estos lineamientos, al reglamento interno de trabajo, así como a las leyes nacionales o internacionales pertinentes. El incumplimiento de esta política puede resultar en la negación de acceso a los sistemas de información de la Organización o a otras acciones disciplinarias o legales.

Es un compromiso de todos los usuarios de **ACESCO**, entender y dar cumplimiento a las políticas consignadas en el presente documento, y acatarlas durante el desarrollo de sus actividades.

5.1. USO PERMITIDO DE LA RED DE DATOS

El uso es permitido primordialmente para asuntos de la Organización. Los sistemas de información de la Organización son únicamente para uso de asuntos relacionados con la misma. El uso personal de los sistemas de información para acceder, descargar, transmitir, distribuir o almacenar **“**Material no permitido”, está prohibido.

El uso personal de herramientas de oficina, tales como Internet, procesadores de texto y hojas de cálculo entre otros, debe ser limitado y bajo ninguna circunstancia el uso personal de estas herramientas debe influir de manera negativa en el desempeño de las tareas y responsabilidades para con la Organización. En los casos en que se haga uso personal excesivo de estas herramientas, la Organización podrá limitar su acceso.

5.2. EQUIPOS DE CÓMPUTO Y PERIFÉRICOS

- Propender por el cuidado y preservación de las herramientas informáticas y computadores asignados al empleado.
- Evitar consumir alimentos y tomar bebidas cerca del equipo asignado. Un incidente de este tipo puede afectar su funcionamiento e incluso dañarlo.
- Evitar colocar elementos pesados sobre el equipo, en especial portátiles ya

que son más frágiles.

- El empleado tendrá la responsabilidad de informar y entregar a la Unidad de Informática los recursos y servicios informáticos que no esté utilizando en su trabajo.
- Los recursos informáticos asignados al empleado están bajo su responsabilidad. En caso de daño, perdida o hurto, el empleado deberá cumplir con los lineamientos establecidos por Gestión Humana.
- En caso de requerir retirar de la empresa cualquier recurso informático no asignado al cargo, es deber del empleado pedir las autorizaciones necesarias.
- Cualquier empleado que sea responsable de un contrato en el cual se involucren computadores, servidores, licencias y periféricos, sean propios o de propiedad de un tercero, debe solicitar autorización a la Unidad de Informática para el uso y transporte de estos dentro de las instalaciones.
- El usuario tendrá la obligación de notificar a través de la mesa de servicio, los traslados de los equipos de cómputo (No portátiles) y periféricos.
- El usuario es responsable de mantener almacenada en su carpeta de OneDrive o Carpeta de Sharepoint, la información resultado de las funciones propias de su rol. Las políticas de retención establecidas por nuestro proveedor de servicios Microsoft, para los elementos eliminados con posibilidad de recuperarlos son: OneDrive: 30 días. Sharepoint Online: 93 días. Correo: 14 días.
- Durante periodos de vacaciones, licencias autorizadas por Gestión Humana, los equipos serán reasignados de manera temporal a quien está ejerciendo las funciones del colaborador ausente. Los usuarios con equipo portátil asignado son responsables de la custodia de este mientras esté vinculado laboralmente a la organización.

5.3. IMPRESIÓN

- Velar porque el servicio de impresión sea utilizado para actividades laborales y uso exclusivo de la organización
- Los usuarios que requieran tener habilitado el servicio de impresión, se le asignará un PIN que debe ser de uso personal e intransferible.
- Propender por el buen uso de las impresoras.
- Realizar un uso razonable del papel e imprimir siempre y cuando sea estrictamente necesario.

- Reportar las solicitudes, requerimientos e incidentes correspondientes al servicio de impresión a la mesa de servicio DeUna.
- Las labores de reparación y/o mantenimiento de las impresoras serán coordinadas por la Unidad de Informática de la organización.

5.4. DISPOSTIVOS DE COLABORACIÓN

- Cualquier dispositivo de colaboración asignado a un empleado, como teléfono, cámara, audífonos, diademas, entre otros, quedará bajo su responsabilidad y deberá ser usado para actividades laborales.
- Ningún empleado está autorizado para retirar, trasladar o modificar los equipos de las salas de conferencia o capacitación sin previo consentimiento por parte de la Unidad de Informática.

5.5. ACCESO A LA RED EMPRESARIAL Y A SUS SERVICIOS

- La Organización asignará a cada usuario una identificación y clave de acceso a los servicios informáticos que éste, por la naturaleza de su cargo, requiera.
- Las identificaciones y claves de acceso a la red empresarial, el Portal Empresarial ALAIA o a cualquier otro Sistema de información son propiedad de la Organización. Estas identificaciones y claves son para uso estrictamente personal e intransferible. La responsabilidad en su manejo recae exclusivamente en el usuario a quién se le asignen. Esta política aplica también para otros factores de autenticación dados por la empresa.
- El acceso a través de conexión VPN para colaboradores nuevos es solicitado por Gestión Humana al equipo de DeUna a través del formato de ingreso, si un colaborador antiguo requiere el acceso, debe solicitarlo al equipo de DeUna a través de correo electrónico, si el acceso es para personal externo a la organización su interlocutor (funcionario Acesco) deberá hacer la solicitud al equipo de DeUna a través de correo electrónico, este acceso se otorga para fines netamente laborales.. El acceso a este servicio es personal e intransferible, Cuando los accesos se otorgan a terceros se debe firmar un documento de responsabilidad.

- El acceso no autorizado a los sistemas de información de la Organización está prohibido. Ningún empleado debe usar la identificación, identidad o contraseña de otro usuario, y de la misma manera ningún usuario debe dar a conocer su contraseña o identificación a otro, excepto en casos que faciliten la reparación o el mantenimiento de algún servicio o equipo y en este caso debe dar a conocer estos datos única y exclusivamente al equipo de soporte técnico de la Organización. En el caso en que este evento se dé, el usuario está en la obligación de cambiar su(s) clave(s) dadas a conocer al equipo de soporte técnico inmediatamente se restablezca el servicio o equipo.
- El usuario no deberá, sin permiso escrito de la Organización, hacer modificaciones a la Red de datos, la Intranet o sus recursos. No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la red. Ante cualquier evento de este tipo la Organización procederá a ejecutar cualquier acción de carácter administrativo, laboral, penal y/o civil que corresponda.
- En la red empresarial no está permitida la operación de software para la descarga y distribución de archivos de música, videos y similares. Cualquier aplicación de este tipo que requiera ser utilizada, deberá ser solicitada a la mesa de servicio DeUna para su evaluación. Adicionalmente, no está permitido almacenar archivos de música, videos y similares de índole personal en el disco duro del equipo asignado al usuario o en su espacio asignado en la nube corporativa.
- El acceso a internet en la Organización debe hacerse desde una estación o dispositivo debidamente registrado y/o autorizado por la Unidad de Informática. Dicho de otra forma, el computador debe estar registrado dentro del DNS (Domain Name Server) primario de la Organización y estar localizado con una dirección IP legítima (validada por la Unidad de Informática). Adicionalmente, se asignan perfiles de navegación al empleado de acuerdo con las funciones que vaya a desempeñar en la organización.

5.6. USO INDEBIDO: PROHIBICIONES EN EL USO DE LAS REDES, LAS COMUNICACIONES ELECTRÓNICAS Y SISTEMAS DE INFORMACIÓN

A continuación, se enuncian las acciones prohibidas en el uso de las redes, comunicaciones electrónicas y sistemas de información. Lo cual es meramente enunciativa más no taxativa, de tal manera que cualquier actividad que, aunque no se encuentre en esta lista, cause perjuicio a los sistemas de información, a las personas o a la empresa, se considerará un uso indebido y estará sujeta a las acciones disciplinarias que la empresa estime conveniente:

- Manipular cualquier dispositivo para ingresar a la red cableada o inalámbrica de la Organización sin la previa autorización de la Unidad de Informática.
- Modificar, desconectar, reubicar o sustraer del lugar donde han sido instalados o configurados, equipos de cómputo, sistemas de información o periféricos sin la debida autorización de la unidad Informática.

- Acceder sin la debida autorización de la Unidad de Informática de la Organización mediante computadores asignados, dispositivos o equipos personales, software, información o redes de ésta, a recursos externos o internos que pertenezcan a la empresa tales como bases de datos, red de datos, red Wireless, sistemas de información, redes externas académicas o de investigación a las cuales esté vinculada **ACESCO**.
- Interferir sin autorización el acceso de otros usuarios a los recursos de los sistemas de información de la Organización.
- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- Utilizar los sistemas de información para propósitos ilegales o no autorizados.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente sin la autorización

escrita del propietario del software.

- Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.
- Usar las comunicaciones electrónicas para acosar o amenazar a los usuarios de la Organización o externos.
- Usar las comunicaciones electrónicas para revelar información privada sin la autorización explícita de la Organización.
- Usar el correo electrónico corporativo para campañas masivas hacia terceros, ya que pueden comprometer la calificación de nuestro dominio como emisor de SPAM.
- Hacer uso de recursos web y servicios de almacenamiento compartidos, que no sean autorizados por la Unidad de Informática.
- Leer la información o archivos de otros usuarios sin su autorización.
- Realizar actividades dentro de una sesión que le pertenece a otro usuario al encontrar la sesión abierta.
- Alterar o falsificar de manera fraudulenta los registros de la Organización, incluyendo registros computarizados, permisos, documentos de identificación, u otros documentos o propiedades.
- Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- Usar las comunicaciones electrónicas para apropiarse de los documentos de otros usuarios.
- Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil, destructiva o intente vulnerar la seguridad de la red informática y sus sistemas de información.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Organización.
- Transportar o almacenar material con derechos de propiedad intelectual o **material no permitido** usando los equipos o las redes de la Organización.
- Utilizar cualquier sistema de información de la Organización para acceder,

descargar, imprimir, almacenar, reenviar, transmitir o distribuir **material no permitido** o correos electrónicos de tipo “cadenas”.

- Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Usar, instalar software de espionaje, monitoreo de tráfico o programas maliciosos en la red de la empresa.
- Instalar, introducir cualquier tipo de programa en la red o equipos sin la debida autorización de la Unidad informática
- Efectuar violaciones a la seguridad o interrupciones de la comunicación de la red. Las violaciones de seguridad incluyen la instalación o utilización de “sniffer”, “floodeos”, “Packet Spoofing”, negación del servicio (DOS), manipulación de ruteo, etc.
- Monitorear o escanear puertos de servidores o switches.
- Evitar o interceptar la autenticación de cualquier usuario por cualquier método.
- Usar cualquier método (exploits, scripts, comandos) para acceder a recursos a los que no se tiene acceso o a áreas protegidas.
- Sustraer cualquier tipo información sensible o confidencial del negocio con fines diferentes a los laborales por medio de dispositivos de almacenamiento extraíble o correo electrónico.

5.7. PRIVACIDAD

- **La privacidad de los usuarios no está garantizada.** Cuando los sistemas de información de la Organización funcionan correctamente, un usuario puede considerar que sus datos generados son información privada, a menos que él mismo realice alguna acción para revelarlos a otros. Los usuarios deben ser conscientes que ningún sistema de información es completamente seguro, por lo cual, personas dentro y fuera de la Organización pueden encontrar formas de tener acceso a la información. De acuerdo con lo anterior, la Organización no puede garantizar la

confidencialidad absoluta de la información almacenada en cualquier dispositivo perteneciente a la empresa y por ende la privacidad de los usuarios.

- **Información clasificada.** Es deber de todo el personal cuidar y proteger la información de carácter confidencial o clasificada como sensible, usando las herramientas que la empresa le proporciona para tal fin.

  El uso de medios removibles y/o Unidades ópticas, para la extracción de información será restringido y solo personal autorizado podrá utilizarlas.

- **Acceso restringido a centro de cableados y datos.** Está prohibido el ingreso a centros de cableados o de datos sin el visto bueno de la unidad de informática.
- **Reparación y mantenimiento de equipos.** El personal de soporte técnico de Informática tiene la autoridad para acceder a archivos individuales o datos cada vez que deban realizar mantenimientos, reparación o chequeo de equipos de computación. Sin embargo, el personal de soporte técnico a cargo de Informática debe garantizar la confidencialidad y custodia en el manejo de la información a la cual tiene acceso y no puede exceder su autoridad en ninguna de estas eventualidades para usar esta información con propósitos diferentes al de mantenimiento y/o reparación.
- **Respuesta al uso indebido de computadores y sistemas de información.** Cuando por alguna causa razonable denominada así por el responsable de la unidad de informática o por quién haga sus veces, se sospeche de algún tipo de uso indebido como se describe en la sección nueve (9) de este documento, la Unidad de Informática puede acceder cualquier cuenta, datos, archivos o servicio de información perteneciente a los involucrados en el incidente, para investigar y de acuerdo a los hallazgos o evidencias dar traslado a la unidad respectiva y/o a la unidad de Gestión Humana, para que éstos de acuerdo al marco de actuación, reglamentos, normas y políticas de la Organización apliquen las acciones respectivas.
- **Monitoreo de la Red empresarial y los Servicios.** Debido a que la Organización se esforzará en mantener la privacidad de las

comunicaciones personales y un nivel de servicio apropiado, la Unidad de Informática monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes. Además, se recolectarán estadísticas de utilización basado en las direcciones de red, protocolo de red y tipo de aplicación. Progresivamente se restringirán usuarios y aplicaciones no esenciales cuando su utilización en la red resulte en la degradación del rendimiento. Tal restricción será notificada a los usuarios a través de los medios apropiados.

5.8. INSTALACIÓN Y USO DE SOFTWARE

- De acuerdo con las normas locales e Internacionales relativas a los derechos de propiedad intelectual, el único software que será instalado en el computador del usuario será aquel que previamente haya sido estandarizado y/o autorizado por la Organización y para lo cual ésta dispone de las licencias respectivas a su nombre.
- El usuario no deberá participar en la copia, distribución, transmisión o cualquier otra práctica no autorizada en las licencias de uso de software.
- El usuario no tiene permitido la instalación de software de “dominio público” o de “distribución libre” (Shareware y Freeware).
- Toda instalación, desinstalación o traslado de software (incluyendo aquellos de “dominio público” de “distribución libre”) desde y hacia un equipo Organizacional debe efectuarse directamente por la Unidad de Informática.
- Cualquier software que se haya instalado en un equipo Organizacional que no cumpla con lo estipulado anteriormente, será desinstalado sin que ello derive ninguna responsabilidad para la Organización.
- Al usar una licencia de software que ha sido instalado en un equipo Institucional o en un equipo Personal, el usuario reconoce los derechos de la Organización anteriormente descritos y es consiente en ellos.
- El uso de programas ejecutables no instalables, conocidos como portables, no deben usarse sin el visto bueno de la Unidad de Informática.

- Está prohibido el uso de software de tipo Anonimato o cualquier otro similar que permita evadir las restricciones de navegación definidas por la organización.

5.9. CORREO ELECTRÓNICO, TEAMS, RED SOCIAL YAMMER Y DEMAS HERRAMIENTA COLABORATIVAS DISPONIBLES

- Todas las políticas incluidas en este documento son aplicables al correo y mensajes electrónicos.
- El correo y mensajes electrónicos debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los grupos de destinatarios, chats y foros de discusión. Las leyes de derechos de autor y licencias de software también aplican para correo electrónico.
- Participar en una cadena de correos es una violación de las Políticas de Uso Aceptable.
- En ningún caso es permitido que un usuario utilice las cuentas o credenciales de identificación que no le han sido asignadas

5.10. RESTRICCIONES SOBRE EL USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTRAÍBLE (TIPO USB)

Con el fin de salvaguardar la información de la organización y evitar cualquier uso indebido que pueda darse a la misma, se han dispuesto las siguientes restricciones para la utilización de dispositivos USB, tales como memorias, discos duros externos, unidades externas de CD/DVD, entre otros que permitan la extracción de información:

- ACESCO se reserva el derecho de permitir el uso de dispositivos de almacenamiento extraíble.
- Los equipos de la organización serán configurados desde el inicio con

restricción para el uso de dispositivos de almacenamiento extraíble. Si para fines laborales, se requiere el uso de algún medio de almacenamiento externo como los ya mencionados, se debe hacer la solicitud a la Unidad Informática, a través de la mesa de servicio para la validación de la necesidad.

- En los equipos de la organización se podrá hacer uso de dispositivos de conexión USB tales como mouse, teclados, y otros que no comprometan la seguridad de la información.

5.11. PAGINAS WEB Y SISTEMA DE MANEJO DE CONTENIDO EN REDES SOCIALES

El responsable de custodiar la Marca e Imagen de la empresa y/o Gerente General de la Unidad de Negocio, acogiendo la directriz organizacional, determinará los estándares para aquellos contenidos considerados como oficiales de la Organización y publicados en su página web. Ninguna otra página o contenido electrónico puede hacer uso de los logos de la Organización sin la autorización expresa del director de la Unidad de Mercadeo o quién haga sus veces.

Los editores de las páginas Web o usuarios que hagan sus veces, que usen información asociada con la Organización deben acogerse a las políticas de la Organización misma, a la ley que las regula incluyendo derechos de autor, leyes sobre obscenidad, calumnia, difamación y piratería de software. El contenido debe ser revisado periódicamente y autorizado por el responsable de custodiar la Marca e Imagen de la empresa y/o Gerente General de la Unidad de Negocio.

5.12. INCUMPLIMIENTO DE LAS POLÍTICAS DE USO RESPONSABLE DE LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMATICOS DE LA ORGANIZACIÓN

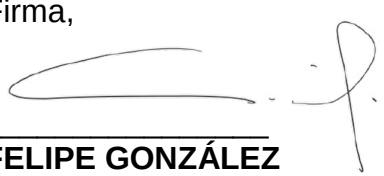
- La Organización hará responsable al usuario de las Políticas y las consecuencias que se derivarían de su incumplimiento. Así mismo, el usuario deberá conocer estas políticas desde su ingreso a la Organización.

- La Organización se reserva el derecho de evaluar periódicamente el cumplimiento de estas *Políticas*. Cualquier acción disciplinaria derivada del incumplimiento de esta, tales como llamadas de atención, suspensiones o despidos, serán consideradas de acuerdo con los procedimientos establecidos por la Organización y en estricto acato del reglamento interno de trabajo y/o las estipulaciones legales vigentes.
- En materia de irregularidades o incumplimiento en el uso del software, el usuario que no cumpla con estas políticas será directamente responsable de las acciones disciplinarias o sanciones por entes externos, que, por la responsabilidad laboral, penal y/o civil se incurra, derivadas de sus propios actos. Igualmente será responsable de los costos y gastos en que pudiera incurrir la Organización derivados de la defensa por el uso no autorizado o indebido de licencias de software. Debido a lo anterior, no es permitido alegar ignorancia ni a estas políticas, ni a la documentación que en las licencias de software se mencione, incluyendo por supuesto las demás licencias en uso.
- En el caso en que razonablemente se asuma que se está haciendo uso ilegal o incorrecto de los servicios informáticos o sistemas de información, la Organización estará en absoluta libertad de limitar o remover las cuentas asignadas sin asumir por ello responsabilidad de ningún tipo.

5.13. REVISIÓN Y MODIFICACIÓN DE LA POLÍTICA

La presente política será revisada siempre que se produzcan hechos significativos que afecten al contenido de esta.

Firma,



FELIPE GONZÁLEZ
Presidente Ejecutivo

6. REGISTRO

N/A.

7. CONTROL DE CAMBIOS

VERSIÓN	MODIFICACIÓN	RESPONSABLE	FECHA
1	Versión original del documento.	Director de informática corporativa.	27-11-2017
2	Modificación del contenido de los ítems 4, 6, 9,10 y 11.	Director de informática corporativa.	27-05-2019
3	-Cambio de razón social e imagen institucional; -Cambia estructura del contenido del documento. --Se incluyen los documentos de referencia.	Director de informática corporativa; Director de Gestión Humana.	25-03-2022
4	Modificaciones: Ítem 5.2: sobre la política de retención de Microsoft. Se incluye en el Ítem 5.10 las restricciones sobre el uso de dispositivos de almacenamiento extraíble tipo USB	Líder Corporativo De infraestructura.	02-05-2022

8. CREACIÓN Y APROBACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
HAROLD GUTIERREZ	**SANDRA PEREIRA**	**FELIPE GONZÁLEZ**
Líder Corporativo De infraestructura. 02-05-2022	Director de informática corporativo. 02-05-2022	Presidente Ejecutivo. 02-05-2022

9. ANEXOS

N/A.

---Fin del Documento---