Políticas de Uso de tecnologías de la Información

1. PROPÓSITO

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

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 **ACECOR**, así como también a aquellos dispositivos de uso personal que ingresen a la misma.

3. TÉRMINOS Y DEFINICIONES

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

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. GENERALIDADES

ACECOR 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, al responsable de Informática o a quien haga sus veces, de los incidentes relacionados con el uso indebido de los sistemas de información.
- **ACECOR** puede restringir o prohibir el uso de sus sistemas de información en cualquier caso en el que se demuestre alguna violación de estas políticas o de alguna ley.
- **ACECOR** 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 están en la obligación de monitorear constantemente los sistemas de información de **ACECOR** a través de las herramientas informáticas disponibles o a través de auditorías externas para responder oportunamente 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.
- 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 **ACECOR**, entender y dar cumplimiento a las políticas consignadas en el presente documento, y acatarlas durante el desarrollo de sus actividades.

5. 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.

6. 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.
- 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 a miembros de la Unidad de Informática 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 a Informática 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 acción 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 previamente autorizada por la Unidad de Informática con el visto bueno del Director/Gerente de área respectivo. 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 de la Organización. 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).

7. 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 dispositivos para ingresar a la red cableada o inalámbrica de la Organización sin la previa autorización de la Unidad de Informática.
- Intentar o modificar, reubicar o sustraer del lugar donde han sido instalados o configurados, equipos de cómputo, sistemas de información o periféricos sin la debida autorización.
- Acceder sin la debida autorización de la Unidad de Informática de la Organización mediante computadores, software, información o redes de la misma, a recursos externos o internos que pertenezcan a la empresa tales como bases de datos, sistemas de información, redes externas académicas o de investigación a las cuales esté vinculada **ACECOR**.
- 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 empresa.
- 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.
- Instalar o usar software de espionaje, monitoreo de tráfico o programas maliciosos en la red de la empresa.
- Introducir cualquier tipo de programa o instalar cualquier software.
- 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.

8. 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.
- **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 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 siete (7) 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.

9. 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.

10. CORREO ELECTRÓNICO, SKYPE EMPRESARIAL, RED SOCIAL YAMMER Y DEMAS HERRAMIENTA COLABORATIVAS DISPONIBLES

- Todas las políticas incluidas en este documento son aplicables al Correo Electrónico.
- El correo electrónico 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.
- Los mensajes de correo electrónico de la Organización en el dominio de la misma deben ser utilizados para uso estrictamente laboral.
- Para hacer una óptima utilización de la capacidad del buzón de mensajes, los mensajes de correo electrónico en los dominios pertenecientes a la Organización, deben ser borrados una vez que la información contenida en ellos ya no sea de utilidad.
- Participar en una cadena de correos es una violación de las Políticas de Uso Aceptable.
- En ningún caso es permitido suplantar las cuentas de usuarios ajenos.

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.

ACEROS CORTADOS S.A.

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 la misma, tales como llamadas de atención, suspensiones o despidos, serán consideradas de acuerdo a 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. En razón de 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 ninguna responsabilidad de ningún tipo.

HUMBERTO FLAVIO HOYOS NARANJO

Director General

Revisión: 11/2017