

CONDICIONES GENERALES DE USO

Requisitos generales para la utilización de los recursos informáticos de la compañía.

Todo usuario debe tener un conocimiento básico de uso de:

- 1.- Sistema operativo Windows en temas como: gestión de carpetas, archivos, copias, navegador, explorador, imprimir.
2. - Ofimática en nuestro caso OFFICE: Word, Excel, Outlook, PowerPoint, OneDrive.

El departamento de Sistemas debe ser plenamente informado de personal contratado que manifieste tener conocimientos especializados de informática así su labor no implique uso de los recursos informáticos de la compañía.

Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de datos de Andina de Seguridad del Valle Ltda. y sus agencias, de acuerdo con las recomendaciones y políticas que en este documento se mencionan.

Los usuarios de la red y equipo de cómputo de Andina de Seguridad del Valle Ltda, deberán solicitar apoyo u orientación al departamento de sistemas ante dudas específicas en el manejo de equipo de cómputo, acceso a la información de los servidores internos y manejo de datos.

El uso de los recursos de cómputo y de la red de datos de Andina de Seguridad del Valle Ltda, tanto en su sede principal Cali, como en sus agencias deberá sujetarse a las siguientes circunstancias:

Los equipos de cómputo y RED Interna solamente podrán ser operados por personal administrativo y/o operativos de Andina de Seguridad del Valle Ltda previamente autorizados por los responsables del equipo, bajo ninguna circunstancia deberán ser operados por personal ajeno a la compañía, se exceptúa las agencias baja coordinación del departamento de Sistemas de Sede principal.

Las actividades realizadas en los equipos de cómputo de la red de datos de Andina de Seguridad del Valle Ltda, en cada uno de sus departamentos y dependencias deberán apegarse a los programas y procesos con fines administrativos de la empresa y no para fines personales u ociosos.

Los equipos de cómputo de Andina de Seguridad del Valle Ltda cuentan con los programas mínimos necesarios para las actividades de oficina, administración e investigación y en caso específico de control y comunicaciones y monitoreo.

Queda prohibido el uso, almacenaje, copiado y reproducción de software sin el consentimiento por escrito del propietario de los derechos de autor o del departamento de sistemas.

El uso de los recursos de cómputo y de la red de datos de Andina de Seguridad del Valle Ltda y sus sucursales conlleva el otorgar crédito de los servicios prestados por la empresa y posiblemente el compartir los beneficios académicos del trabajo, previo acuerdo con el responsable de cada proyecto.

USOS ACEPTABLES DE LOS RECURSOS DE CÓMPUTO Y RED DE DATOS DE ANDINA DE SEGURIDAD DEL VALLE LTDA Y AGENCIAS

Algunos usos aceptables de los recursos de cómputo y red de datos de Andina de Seguridad del Valle Ltda y sus agencias contemplan:

- Funciones de oficina e investigación apoyada en el uso de recursos de software.
- Atención de clientes a través del uso de la computadora.
- Generación de documentos e informes y material de la compañía.
- Montaje de interfaces apoyadas en equipos de cómputo para medir, regular, retroalimentar y/o analizar procesos, funciones, dependencias y tareas específicas por departamento o dependencia.
- Actividades de gestión y administración que requiera el uso de medios electrónicos y sistemas distribuidos.

Los usuarios deberán tener bien definidas las actividades que van a realizar con los equipos de cómputo y red de datos de Andina de Seguridad del Valle Ltda, esto repercutirá en un mejor desempeño y optimización de los recursos de cómputo de la compañía.

RESTRICCIONES Y RECOMENDACIONES A LOS USUARIOS

Todos los usuarios deberán respetar la integridad de los equipos de cómputo y periféricos de Andina de Seguridad del Valle Ltda y sus agencias, además de la confidencialidad y los derechos individuales de los demás, a continuación se describen el propósito de las políticas y los lineamientos de seguridad definidos por la compañía:

GESTION DE ACTIVOS

- Evitando conectar y/o desconectar componentes de hardware de los equipos de cómputo, ante cualquier falla de los equipos es necesario reportarla a los responsables en turno para que solucionen el desperfecto.
- Absteniéndose de consultar material inapropiado, sacrílego, difamatorio, obsceno, pornográfico, de violencia explícita, indecente, ilegal o cualquier otro tipo de material que pudiera ofender a los usuarios de espacios de cómputo comunes.
- Absteniéndose de realizar actividades ociosas (Juegos, Chat, descarga de música y software y otras actividades que saturan el ancho de banda de la red interna de Andina de Seguridad del Valle Ltda). Bajo ninguna circunstancia la infraestructura de cómputo deberá ser utilizada para lanzar ataques a otros equipos conectados en red.
- Evitando monitorear con algún tipo de software o medio el contenido de los equipos de cómputo y las consultas o envío de información de otros usuarios de la red de datos de Andina de Seguridad del Valle Ltda.
- Respetando la configuración original de los equipos en cada una de las oficinas, evitando personalizar el aspecto y contenido de los mismos, así como la instalación de cualquier tipo de software ajeno al instalado por el personal encargado del área.
- Los equipos de cómputo no podrán ser trasladados del sitio asignado inicialmente, ni cambiar de funcionario al que le fue asignado, sin previo aviso al Dpto. de Sistemas.
- El Dpto. de Sistemas es la única área autorizada para hacer instalación de software y controlar las licencias de programas instalados en los equipos de la entidad.
- Está prohibido que personal ajeno al Dpto. de Sistemas destape o retire partes de los equipos de cómputo de la compañía.

- Está prohibido conectar modem o celulares para acceder a Internet, dentro de la red LAN de la entidad.

GESTION DE USUARIOS

- Los funcionarios que ingresen a Andina de Seguridad del Valle deberán solicitar a Talento Humano o Jefe Inmediato que se envíe un correo al Dpto. de Sistemas para la asignación de claves de acceso a las aplicaciones corporativas, uso de la red y correo electrónico.
- El Dpto. de Sistemas es el responsable de crear todos los usuarios en las aplicaciones corporativas, correo electrónico, dar acceso a la red de datos, esto se realiza cuando se envíe el correo de autorización por parte de Talento Humano o Jefe Inmediato.
- Cuando el funcionario se retira de la entidad ya sea por vacaciones, renuncia o retiro definitivo es responsabilidad de Talento Humano, solicitar al Dpto. de Sistemas la desactivación del usuario en todas las aplicaciones, accesos a la red corporativa y correo electrónico.

CONTROL DE ACCESO A LOS SISTEMAS

Con el fin de controlar el acceso a los sistemas de información de Andina de Seguridad del Valle, se ha definido la creación de usuarios y perfiles, de acuerdo con las labores desempeñadas por cada funcionario.

- Cada usuario es responsable exclusivo de mantener a salvo la contraseña de ingreso al equipo asignado. Los usuarios autorizados a acceder a los sistemas de información de la compañía, son responsables de la seguridad de las contraseñas y cuentas de usuario. Las contraseñas son únicas e intransferibles.
- No se podrá guardar o escribir las contraseñas en papeles o algunas superficies, así como dejar constancia de ellas.
- La contraseña asignada para el acceso a los sistemas de información no deberá contener característica personales o de los parientes, como fechas de cumpleaños o alguna otra fecha importante. Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números y mínimo ocho (8) caracteres.
- La contraseña inicial emitida a un nuevo usuario, sólo debe ser válida para la primera sesión y posteriormente debe cambiarse por seguridad.

- El usuario es responsable de custodiar los accesos a las aplicaciones, la información y herramientas tecnológicas suministradas por parte de la compañía.
- Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.
- Está prohibido intentar violar los sistemas de seguridad y de control de acceso a los sistemas de información.
- Para desbloquear la clave de acceso, el usuario deberá realizar la solicitud ante el Dpto. de Sistemas, dicho desbloqueo se hace posterior a la identificación positiva.
- Las contraseñas tendrán una validez de 60 días calendario, cumplido este tiempo el sistema solicitará el cambio, sino se realiza el cambio, no permitirá el acceso al sistema.

ACCESO A LA NAVEGACION EN INTERNET

- Se prohíbe el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.
- Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red de la compañía, no se permite el envío y descargas de información masiva como música, videos y software no autorizado.
- Los funcionarios no deben descargar programas maliciosos o demos, esto con el objeto de salvaguardar la información de Andina de Seguridad del Valle Ltda contra usos no autorizados, divulgación, modificación, daño o pérdida.
- Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso.

ESCRITORIO Y PANTALLA

- Al imprimir documentos de carácter confidencial, éstos deben ser retirados de la impresora inmediatamente.

- Los computadores cargarán por defecto el fondo de pantalla, el cual no podrá ser modificado y deberá permanecer activo.
- El funcionario de Andina de Seguridad del Valle debe bloquear la pantalla de su computador cuando por cualquier motivo se ausente del puesto de trabajo.
- Los usuarios son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia.
- Al finalizar sus actividades, los usuarios deberán verificar que en sus puestos de trabajo no quede expuesta información crítica o sensible para la compañía.
- Se prohíbe el almacenamiento de información personal en los computadores de la compañía.

USO DE CORREO CORPORATIVO

- La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la compañía.
- El correo electrónico corporativo se debe utilizar estrictamente como herramienta de comunicación de la compañía; esto es para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo desempeñadas.
- El correo electrónico corporativo es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.
- Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas y datos de la compañía.

- El usuario deberá notificar cualquier recibo de correo sospechoso, a las cuentas informatica@andinaseguridad.com.co – informatica1@andinaseguridad.com.co . El correo sospechoso no debe ser abierto ni reenviado a ningún usuario.

POLITICA DE RESPALDO Y RESTAURACION

- La información laboral sensible y crítica de cada usuario debe ser almacenada en la herramienta de OneDrive.
- Cada usuario es responsable de los controles de acceso que le otorga a la información para que sea consultada por otros funcionarios.
- Los funcionarios son los únicos responsables de salvaguardar la información local del equipo en la herramienta de OneDrive.
- La información que no se encuentre en la herramienta de OneDrive y por algún motivo o circunstancia se extravié será responsabilidad de cada colaborador.

SERVIDORES Y EQUIPO DE CONECTIVIDAD

Los servidores y equipo de conectividad de la red de datos de Andina de Seguridad del Valle Ltda y sus agencias deberán ubicarse en un área física que cumpla las recomendaciones para un centro de telecomunicaciones:

- Acceso restringido.
- Temperatura adecuada.
- Protección contra descargas eléctricas.
- Mobiliario adecuado que garantice la seguridad de los equipos.

El departamento de sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la red de datos de Andina de Seguridad del Valle Ltda. Así mismo es responsable de llevar a cabo un monitoreo constante de los servicios y posibles fallas de red y de administrar los recursos de conectividad de la oficina principal y las agencias.

Bajo ninguna circunstancia los equipos de conectividad (Switches, ruteadores, cableado estructurado, firewall, servidores, etc) podrán ser operados por personal ajeno al departamento de sistemas de Andina de Seguridad del Valle Ltda).

La instalación y/o configuración de todo servidor conectado a la red de datos de Andina de Seguridad del Valle Ltda deberá ser autorizada por el departamento de sistemas. Durante la configuración de los servidores conectados a la red de datos de Andina de Seguridad del Valle Ltda los administradores de la red deberán normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

Queda totalmente prohibida cualquier actividad de intrusión para manipular la configuración de los servidores de red y equipo de conectividad propiedad de Andina de Seguridad del Valle Ltda. Cualquier actividad con estos fines provocará el cese inmediato de los servicios prestados y el procedimiento legal correspondiente.

Andina de Seguridad del Valle Ltda se reserva el derecho para modificar o incluso suspender el servicio o partes del mismo cuando sea necesario, por razones administrativas, de mantenimiento de los equipos o por causas de fuerza mayor, avisando con anterioridad a los usuarios de estos movimientos.

ADVERTENCIA y/o PRECACUCIONES

- La no aplicación de las normas y políticas descritas en este documento podrá acarrear a los infractores sanciones disciplinarias, de acuerdo a lo establecido en el reglamento interno de trabajo de la compañía.
- No exponer a la PC a los rayos del sol.
- No colocar a la PC en lugares húmedos.
- Mantener a la PC alejada de equipos electrónicos o bocinas que produzcan campos magnéticos ya que pueden dañar la información.
- No fumar cerca de la PC.

- No comer y/o beber cerca del Equipo de Cómputo.
- Usar “No-Break” (UPS) para regular la energía eléctrica y por si la energía se corta que haya tiempo de guardar la información.
- Adecuar la instalación eléctrica de la casa u oficina mediante un especialista como pre requisito para permitir instalación de un equipo en responsabilidad de Andina de Seguridad del Valle Ltda.
- No abrir documentos adjuntos que genere sospechas de su procedencia.
- Escanear memorias USB con el antivirus al introducirlas al computador.
- Cuando se requiera instalar un software o programa nuevo, debe consultar y contar con la autorización del departamento de sistemas y el jefe inmediato.
- La instalación del software debe realizarse por el personal de sistemas.
- Hacer adecuado uso de los recursos tecnológicos solo para la operación de Andina de Seguridad del Valle Ltda. y no para uso personal.

Atentamente:

Elaboro:

Gerente General

Administrador de Sistemas

Elaboro:

Revisado:

Administrador de Sistemas

Gerente Nacional de Calidad