MANUAL DE INFORMATICA Y POLITICAS DE SEGURIDAD DE LA INFORMACION

AGUAS DE BARRANCABERMEJA S.A. E.S.P.

CONTROL DE CAMBIOS		
VERSION	**FECHA DE APROBACION**	**DESCRIPCION DEL CAMBIO**

	ELABORADO POR	**REVISADO POR**	**APROBADO POR**
Cargo	Profesional III adscrito a la Subgerencia Administrativa y Financiera	Subgerente Administrativa y Financiera	Gerente
Nombre	Rafael Andrés Lastre G.	Carolina Gómez Peñaloza	Sergio Amaris Fernández
Firma			
Fecha	Junio de 2014	Julio de 2014	12-02-2015

CONTENIDO

Comité:
Equipo integrado por la Gerencia, el Gestor de Seguridad, los Jefes de área y el personal administrativo de la Empresa (ocasionalmente) convocados para fines específicos como:

- Adquisiciones de Hardware y software
- Establecimiento de estándares de la Empresa tanto de hardware como de software.
- Establecimiento de la Arquitectura tecnológica de grupo.
- Capacitar a los empleados en lo relacionado con las Políticas de Seguridad.

Contraseña:
Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

Gestor de Seguridad:
Persona dotada de conocimientos técnicos, encargada de velar por la seguridad de la información, realizar auditorías de seguridad, elaborar documentos de seguridad como, políticas, normas; y de llevar un estricto control referente a los servicios prestados y niveles de seguridad aceptados para tales servicios. Este rol es asumido por el Profesional de Tecnología.

Red:
Equipos de cómputo, sistemas de información y redes de telemática de la Empresa.

Responsable de Activos:
Esta persona debe mantener el inventario físico al día, velar por que todos los activos tengan sus respectivas pólizas de seguros bajo los parámetros entregados por la Gerencia.

Solución Antivirus:
Recurso informático empleado para solucionar problemas causados por virus informáticos.

Usuario:

Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por la Empresa tales como equipos de cómputo, sistemas de información, redes de telemática.

Virus informático:
Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

POLITICAS DE SEGURIDAD DE LA INFORMACION

RESPONSABILIDADES

PRIMERO: Responsabilidad en distintos grados, a:

Comité de Seguridad de la Información. El comité está encargado de recomendar la formulación y actualización periódica de las políticas relativas a los recursos informáticos y a la seguridad de la información. La Gerencia, Subgerentes y Profesional de recursos informáticos de la Empresa. Es responsable de clasificar y proteger la información utilizada por ellos; cuando ocurra un incidente grave que refleje alguna debilidad, deberán tomar las acciones para reducir los riesgos.
Control de Gestión. Debe velar por el cumplimiento de las políticas, normas y procedimientos de seguridad de la información en la Empresa. Igualmente, advertir acerca de las vulnerabilidades detectadas.
Profesional de Recursos Informáticos. Responsable de implantar las políticas, normas y procedimientos de seguridad en la empresa; evaluar, proponer la adquisición e implantar productos de seguridad informática; acordar el análisis de riesgos, planes de contingencia y realizar las demás actividades necesarias para garantizar un ambiente informático seguro.
Así mismo es responsable por la planeación y ejecución del mantenimiento preventivo y correctivo de los computadores e impresoras, de acuerdo con los procedimientos establecidos.

El Administrador del sistema. Es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y llevar a cabo las tareas de seguridad relativas a los sistemas que administra.

Usuario. Todo servidor público o persona que asuma funciones públicas, es responsable de cumplir con todas las políticas informáticas y de seguridad de la Empresa.

DERECHOS MORALES Y PATRIMONIALES

Los usuarios son responsables de la custodia y la confidencialidad de los datos y la información a la cual tengan acceso en forma directa e indirecta.
La empresa es propietaria de todos los datos e información que circule o se genere al interior de la misma o que esté disponible a través de sus sistemas de información y/o computadores.
En este sentido, el Gerente y Servidores públicos de nivel directivo clasificaran los datos y la información generados o utilizados por su Subgerencia solicitando a sus colaboradores y contratistas seguir los procedimientos establecidos por la Subgerencia Administrativa y Financiera para el resguardo de los mismos a través de copias de seguridad (Backup).

DIVULGACION DE LA INFORMACION

Entregar a los grupos de interés información acerca de la gestión de la Empresa, a través de los informes de corte de ejercicio.
Las solicitudes de información se entregaran de acuerdo con los lineamientos o plazos definidos, la regulación o la ley, a través de los servidores públicos de nivel directivo responsables de los procesos o por el que se delegue para tal fin.
La información entregada a los medios de comunicación debe hacerse a través del funcionario encargado del manejo de la comunicación empresarial.
La empresa no se hace responsable por las consecuencias que se deriven de la utilización inadecuada por parte de terceros. Igualmente, se abstiene de suministrar la información que haya recibido de terceros para su uso interno y confidencial.

INFORMACIÓN CONFIDENCIAL

Exigir a los usuarios la protección de la información clasificada como confidencial o de uso restringido.

Incluir una cláusula de confidencialidad en los contratos u órdenes, cuando el contratista requiera acceder de manera directa o indirecta a los datos o información de la Empresa.
Todo empleado que participe en proyectos de la Empresa, o tenga acceso a su información, debe guardar confidencialidad sobre la misma. El responsable del proyecto debe solicitar a los participantes, como parte de los términos, compromiso y condiciones iniciales de su participación, que firmen un acuerdo de confidencialidad de la información.
Se prohíbe la extracción de datos confidenciales, sin la aprobación previa de la gerencia o la Subgerencia respectiva.

RECURSOS INFORMÁTICOS

Establecer el cambio periódico de los recursos informáticos, dependiendo de la obsolescencia, la vida útil, el estado de los mismos y las necesidades de la Empresa.
Se dará de baja a los equipos teniendo en cuenta el procedimiento establecido para tal fin.
Exigir a los usuarios la utilización responsable y razonable de los recursos informáticos. Igualmente, el acatamiento de las medidas de control establecidas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde con la importancia de los datos y la naturaleza de los riesgos.
Solicitar al usuario el cuidado de los recursos informáticos, suministrados para el cumplimiento de sus responsabilidades. Con un debido proceso la empresa podrá cobrar o pedir al usuario la reposición de los equipos cuando se compruebe que el daño fue dolorosamente causado por este.
Exigir que los equipos informáticos se marquen para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
No pueden moverse o reubicar los equipos de escritorio sin la autorización de la Subgerencia Administrativa y Financiera.
La pérdida o hurto de los recursos informáticos debe ser informado inmediatamente a la Subgerencia Administrativa y Financiera.

ADMINISTRACIÓN Y CONTROL

La conexión a la red debe ser autorizada por el Profesional de Recursos Informáticos con las directrices emitidas por la Subgerencia Administrativa y Financiera. No pueden conectarse computadores, servidores, hubs, switches, routers, o cualquier otro hardware a la red sin la autorización correspondiente.

Autorizar al administrador del sistema para solucionar los problemas y/o realizar mantenimientos preventivos y correctivos de los recursos informáticos conectados o no a la red, previa concertación con el usuario de los mismos.
Reservar al Administrador del sistema el derecho de desconectar usuarios o recursos informáticos que puedan vulnerar la seguridad.
Los usuarios son responsables de ayudar a mantener la seguridad de la red siguiendo los procedimientos establecidos. Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente a Profesional de Recursos Informáticos adscrita a la Subgerencia Administrativa y Financiera.
Autorizar al Administrador del sistema para supervisar el uso que hacen los usuarios en internet (por ejemplo, trafico, páginas visitadas, horas pico, etc.) el tamaño de los buzones de correo electrónico, utilización de las impresoras y demás recursos informáticos, sin que se vulnere el derecho a la privacidad.
El profesional de recursos informáticos o quien haga sus veces es responsable de instalar un antivirus en todos los computadores de escritorio, portátiles y servidores de la empresa.
Los usuarios deben mantener activo el antivirus; permitir la instalación de las últimas versiones, de acuerdo con las instrucciones de la Subgerencia Administrativa y Financiera, y realizar chequeos periódicos.
En caso de detectar alguna infección, se deberá avisar de inmediato al Profesional de Tecnología para evitar o controlar su posible diseminación.

WEBSITE E INTRANET

Adoptar el Website http://www.aguasdebarrancabermeja.gov.co y la intranet como los sitios electrónicos oficiales de la empresa, para la publicación de información externa e interna.
La inclusión de Patrocinadores en la intranet o página web de la empresa estará sujeta a los convenios y/o acuerdos empresariales previamente establecidos.
Realizar la publicación de información en la Website e intranet con la autorización de la Subgerencia Administrativa y Financiera y ejecutado por el administrador de la Web o quien haga sus veces, pero tratándose de información sobre la actividad contractual de la empresa, la misma deberá ser remitida por la secretaria general. Cuando la información a publicar sea inherente a alguna Subgerencia específica, deberá el Subgerente o la Gerencia enviar dicha autorización. Una vez publicada, la actualización es responsabilidad del funcionario solicitante.

DERECHOS DE AUTOR LICENCIAS DE SOFTWARE

Proteger el Derecho de Autor y Derechos Conexos, de acuerdo con lo consagrado en la constitución política, los ordenamientos legales y acuerdos regionales.
Emplear, en lo posible, las últimas versiones del software disponible en el mercado, para disminuir los problemas ocasionados por las diferencia de versiones.
Todos los programas utilizados en los computadores de la empresa deben contar con sus respectivas licencias de uso vigentes y condiciones exigidas
Si alguna persona de la empresa Instala software no autorizado será bajo su responsabilidad y deberá asumir las consecuencias que esto representa, conforme a las diversas leyes aplicables por violaciones a la propiedad intelectual.

CORREO ELECTRONICO

La empresa suministrara el acceso al correo electrónico y a internet, como herramientas para la realización de las labores, dependiendo de las responsabilidades y naturaleza del trabajo contratado, conforme a lo previsto en el manual de funciones.
El uso inadecuado de internet constituirá una falta grave, que se clasificara como tal por la magnitud del hecho o por no atender los requerimientos de la empresa para que se cese la utilización indebida. La comprobación y las sanciones disciplinarias se realizaran conforme lo establecido en la legislación aplicable.
Se establecen como comunicaciones oficiales todos aquellos mensajes o correos que son recibidos y enviados a través de las cuentas institucionales.
Responsabilizar, a los usuarios, de revisar su correo y atender los compromisos definidos por este medio.
El Profesional de recursos informáticos o quien haga sus veces es responsable de asignar un espacio determinado para cada buzón del correo electrónico.
El usuario tendrá la responsabilidad de realizar copias de seguridad (backups).

Prohibir expresamente el envío individual o masivo de propaganda gremial, religiosa o política; alertas falsas de virus; cadenas de mensajes que ofrecen dinero; difamaciones contra empresas o personas, mensajes de publicidad no solicitados y, en general, en todas las publicaciones y documentos que atenten contra los valores institucionales o la moral pública.
La Profesional de Recursos Informáticos es responsable de impartir las instrucciones requeridas por los usuarios para utilizar el correo. Así mismo

deberá implementar los mecanismos de seguridad, control y estadísticas de utilización del mismo.
Todos los usuarios deberán tener el nombre y/o el logo (Firma) de la empresa en documentos electrónicos autorizados o que la empresa considere oficiales.

GESTIÓN DOCUMENTAL

Propender porque las circulares y en general comunicaciones informáticas enviadas entre los servidores de la Empresa Aguas de Barrancabermeja S.A E.S.P, se realice por medios electrónicos.
PARÁGRAFO: La empresa acoge lo estipulado en la ley de comercio electrónico (Ley 527 de 1999)
Optimizar la impresión de memorandos y suprimir los archivos físicos que se deseen conservar como acuse de recibo o consulta de los documentos enviados a través del correo electrónico y sus aplicaciones, exceptuando aquellos cuyo destino sea serie y subseries documentales contratos, carpetas de órdenes de compra, carpetas de órdenes de servicio, carpeta de hojas de vida, carpetas de reembolso de caja menor, actas de junta directiva, actas de asamblea general de accionistas, actas de remisión de gerencia, actas de los comités de contratación y gerencia, contratos o documentos de origen legal. En estos casos se imprimirá solamente un original que reposa en dichas carpetas.
Conservar la correspondencia interna y externa (recibida y enviada) en medio magnético, para evitar en lo posible la impresión de copias.
Todas las actividades referentes de gestión documental de la empresa, estarán sujetas a los procedimientos establecidos en el manual de archivo y correspondencia aprobado en el comité mediante acta 001 de 2007 o a las modificaciones que al respecto se dicten.
Se establece como comunicaciones oficiales todas aquellas que son recibidas y enviadas a través del Sistema de Gestión Documental Mercurio.
Responsabilizar al funcionario de mantener consultando permanente la cuenta habilitada en el Sistema de Gestión Documental Mercurio y atender los compromisos definidos por este medio.
Cualquier comunicación registrada por otro medio, no será considerada como oficial y el funcionario responderá por las consecuencias derivadas de ello, todo documento será reconocido una vez haya sido enviado a su destinatario, el radicado de por sí solo no implica oficialización del documento y se entenderá por no tramitado, el funcionario que a sabiendas radique y no envié la comunicación responderá por las consecuencias que se deriven de dicho acto.

Solamente se exceptuarán situaciones que por dificultades del sistema o fallos en las redes no permita hacer en debido registro con el sistema de gestión documental, lo que sí requeriría un registro manual y ser certificado por la persona competente.
La radicación de correspondencia interna y externa que requiera imprimirse es responsabilidad de cada dirección y la oficina de gestión documental únicamente se encargara del envío local y/o nacional.
Las copias de respaldo de mensajes, datos y confirmaciones de entregan serán responsabilidad de cada usuario.

SEGURIDAD PARA COMPUTADORES, SERVIDORES Y REDES

Prohibir a los usuarios la modificación de la configuración de hardware y software establecida por el funcionario encargado de administrar el sistema.
Se exceptúan a los usuarios de equipos portátiles que deban utilizar el equipo en lugares diferentes a los de la empresa.
La Subgerencia administrativa y financiera será responsable que los equipos se protejan para disminuir el riesgo de hurto, destrucción, fluctuaciones de energía, incendio y medio ambiente (por ejemplo: agua), utilizando instalaciones en condiciones adecuadas, cerraduras, vigilantes, protectores contra transitorios de energía eléctrica y, para los servidores, fuentes de poder interrumpibles (UPS).
No está permitido conectar a la red informática de la empresa computadores portátiles ajenos y, en caso de ser necesario, se requiere solicitar la autorización correspondiente al Profesional de Recursos Informáticos o quien haga sus veces para la configuración.
Prohibir el uso de módems en computadores que tengan conexión a la red local (LAN), para prevenir la intrusión de hackers a través de las puertas traseras. Todas las comunicaciones de datos deben efectuarse a través de la red LAN de la empresa.
Se exceptúan los equipos que están debidamente autorizados o que se utilizan para realizar pagos. En estos casos, la conexión se realizara por el tiempo necesario.
El administrador del sistema o quien haga sus veces es responsable de tomar copias de respaldo de los datos guardados en los servidores. Las copias de seguridad deben guardarse en un lugar seguro y, las de los servidores de misión crítica, enviarse para almacenamiento externo con una copia a la Subgerencia administrativa y financiera.

CUENTAS DE LOS USUARIOS

Exigir que la solicitud de una nueva cuenta o el cambio de privilegios se haga a través del funcionario encargado de la Subgerencia.
Cuando la empresa vincula a un respectivo funcionario este debe firmar un documento donde declara conocer las políticas informáticas y de seguridad de la información y acepta las responsabilidades.
No debe concederse una cuenta a personas que no sean empleados de la empresa, a menos que estén debidamente autorizados por la Subgerencia correspondiente. En este caso, la persona debe firmar un documento donde declare conocer las políticas informáticas y de seguridad de la información y acepta sus responsabilidades.
No debe otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto, a menos que se determine la necesidad. En todo caso, esa facilidad solo debe habilitarse para el periodo requerido o para efectuar el trabajo (como por ejemplo, el mantenimiento remoto), con acompañamiento y/o supervisión del administrador del sistema. Si hace falta una conexión remota durante un periodo más largo, entonces, se debe usar un sistema de autenticación más robusto.
Prohibir el uso de cuentas en las que no se identifican el usuario asignado (anónimas). Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.
Toda cuenta debe quedar automáticamente suspendida después de determinado periodo de inactividad.
Periódicamente, los privilegios concedidos a los usuarios deben ser ratificados por las personas que los autorizaron.
El área de Gestión Humana debe informar a los usuarios que cesan en sus funciones.

IDENTIFICACION, CONTRASEÑAS Y AUTORIZACIONES

Todos los usuarios que acceden a los sistemas de información requieren de un único e intransferible identificador, el cual será proporcionado como parte del proceso de autorización.
Los identificadores concedidos deberán eliminarse o deshabilitarse, por solicitud de la Subgerencia, cuando cese la vinculación del usuario con la empresa en forma permanente o temporal, o cuando se presente un uso indebido.
De esta manera, todas las acciones realizadas con un identificador de usuario son responsabilidad del titular del mismo.
Responsabilizar a los usuarios por la confidencialidad de la contraseña utilizada en los sistemas de información,

El Administrador del Sistema o quien haga sus veces debe configurar el tiempo de vigencia y la longitud mínima de las contraseñas utilizadas en los sistemas de información.
Los usuarios que tengan contraseña, tanto al iniciar el computador como en los archivos pertenecientes a la empresa, deberán entregarlas al superior inmediato cuando estén en vacaciones para utilizarlas en caso de requerirse.
Solicitar al usuario que no escriba su contraseña. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares o contraseñas previamente empleadas. Siempre que sea posible se debe impedir que los usuarios vuelvan a usar contraseñas anteriores.
Exigir que la contraseña inicial, emitida a un nuevo usuario, solo sea válida para la primera sesión, En ese momento, el usuario debe escoger otra contraseña.
Las contraseñas predefinidas que traen los equipos nuevos deben cambiarse inmediatamente entre en funcionamiento.
Prevenir el acceso no autorizado, mediante el uso de un sistema de contraseñas con parámetros de complejidad. En los datos compartidos debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de leer, escribir, modificar, crear, o borrar datos importantes por parte de personas no autorizadas. Estos privilegios deben definirse de una manera consistente con las responsabilidades del usuario.

SEGURIDAD FISICA Y DEL ENTORNO

Implantar los controles de seguridad apropiados para el ingreso a las instalaciones de la empresa de funcionarios, contratistas y terceros.
El acceso de personal contratista, se debe autorizar una vez se haya formalizado el contrato y de acuerdo con los controles de seguridad definidos.
Se debe exigir al personal contratista, cumplir igualmente con las políticas, procesos procedimientos establecidos en la empresa.
En caso de requerirse, los colaboradores que tengan equipos portátiles de la Empresa, deben permitir la revisión y registro de los equipos, tanto al ingresar como al salir de las dependencias de la Empresa.
Todo contratista encargado del mantenimiento de equipos de informática, debe identificarse, hacer los registros correspondientes, enseñarles a los vigilantes la autorización de la salida o ingreso de cualquier equipo, caso contrario, no se autoriza.
Las áreas de acceso restringido deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado.

Solicitar a los usuarios de los sistemas de información que se reporte a la Subgerencia Administrativa y Financiera sobre cualquier debilidad en la seguridad, observada o sospechada, o amenaza a las instalaciones o los sistemas.
Se prohíbe a los usuarios intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Empresa.

FALTA Y SANCIONES DISCIPLINARIAS

Considerar falta leve:
Desatender la revisión periódica del correo electrónico y/o sistemas de información que maneje la empresa, y no cumplir con los compromisos definidos por este medio.
Utilizar cualquier recurso informático para propósitos comerciales no autorizados, ganancia personal o incumplimiento de cualquier disposición legal vigente.
Cobrar a terceros por el uso el acceso a los servicios de la Red, sin que exista un contrato y autorización formal.
Instalar hardware y/o software sin la autorización de la Dirección Administrativa y Financiera y/o utilizar software comercial ilegalmente copiado, incluyendo textos, imágenes gráficas o grabaciones de audio o video.
Divulgar o remover información, software, impresiones o medios magnéticos sin el explícito permiso del propietario.
Considerar falta grave:
Usar sin autorización identificadores de usuario o cuentas u otras formas de acceso a Recursos informáticos de la Red.
Utilizar la Internet, los sistemas de información de la empresa o el correo propio o de otro empleado con fines de engaño o fraude para divulgar información confidencial de la empresa.
Crear, utilizar o distribuir programas que puedan dañas los datos, archivos, aplicaciones o impidan el adecuado funcionamiento de la Red.
Utilizar, capturar o desencriptar contraseñas y/o protocolos de comunicaciones de otros usuarios o terceros, excepto cuando exista un procedimiento establecido para casos de emergencia o fuerza mayor o sea autorizado.
Alterar el software o la configuración del hardware de cualquier computador, agregar cualquier dispositivo sin el permiso de la Subgerencia Administrativa y Financiera y acceder a programas y archivos compartidos sin autorización.
Enviar anónimos desde o hacia internet, el correo propio o de otro servidor.

Utilizar técnicas y/o herramientas de ataque informático desde y hacia la empresa.

Las disposiciones incluidas en este documento son un marco de referencia para los usuarios y aplican por igual a todas las personas que tengan acceso a los sistemas o información de la empresa.
En el caso de los empleados, el procedimiento para comprobación de las faltas y las sanciones disciplinarias a aplicar, se rigen por lo establecido en el Reglamento interno de trabajo vigente o en la ley.
En el caso de los contratistas, la infracción de las normas y políticas de informática y seguridad, se consideran como un incumplimiento del contrato, que podrá dar lugar a la terminación del mismo, sin perjuicio de las demás acciones o que haya lugar.

PROCEDIMIENTOS DE GESTION INFORMATICA

GIF-PR-001 PROCEDIMIENTO ASIGNACION DE PERMISOS PARA LOS SISTEMAS DE INFORMACION

GIF-PR-002 PROCEDIMIENTO SOLICITUD DE SERVICIO DE SOPORTE DE USUARIOS

GIF-PR-003 PROCEDIMIENTO MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE CÓMPUTO.

Anexos

Anexo 1. Formato Checklist Aplicaciones e Información
Anexo 2. Formato Hoja de Vida Equipos de Computo
Anexo 3. Formato Acta de Entrega y Recepción de Equipos
Anexo 4. Formato Solicitud de Soporte Usuario
Anexo 5. Manual de Usuario Copias de Seguridad de los Sistemas de Información