LISTA DE DISTRIBUCIÓN

CARGO
Coordinador del S.G.C

-ORIGINAL FIRMADO-

ELABORÓ:	REVISÓ:	APROBÓ:
Director Técnico	Director Técnico	Director Técnico

1. OBJETIVOS.

El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información del CDA.

Difundir las políticas y estándares de seguridad informática a todo el personal del CDA , para que sea de su conocimiento y cumplimiento en los recursos informáticos utilizados o asignados.

2. ALCANCE

El documento describe las políticas y los estándares de seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos CDA.

3. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

3.1 Política

Todo usuario de bienes y servicios informáticos debe firmar un convenio en el que acepte las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información del CDA, así como el estricto a pego al *presente manual*.

3.2 Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las *Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.*

3.3 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos del CDA deben firmar de aceptación el convenio de confidencialidad y uso adecuado de los recursos Informáticos y de información del CDA, así como comprometerse a cumplir con lo establecido en el Manual de *Políticas y Estándares de Seguridad Informática para Usuarios.*

3.4 Entrenamiento en seguridad informática

Todo empleado del CDA de nuevo ingreso deberá de contar con la inducción sobre el *Manual de Políticas y Estándares de Seguridad Informática para Usuarios,* a través de la Gerencia General donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

3.5 Medidas disciplinarias.

Cuando alguno de los Directivos o de los empleados detecte el incumplimiento al presente manual, informará a la Gerencia General para que se tomen las medidas correspondientes.

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial del CDA, o de que sele declare culpable de un delito informático.

4. ESTÁNDARES QUE SE REQUIERENCON RESPECTO A LA SEGURIDADFÍSICAY AMBIENTAL DE LA INFORMACION

4.1 Política

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del CDA, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y el centro de cómputo del CDA.

El CDA, se encargará de proteger y garantizar que los recursos del sistema de información (Aplicaciones y Bases de Datos) y Registro, se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite.

4.2 Resguardo y protección de la información

El usuario deberá reportar de forma inmediata a su jefe inmediato o a la Gerencia, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

El usuario tiene la obligación de proteger los discos, disquetes, cintas magnéticas, CD-ROM y otros medios magnéticos de almacenamiento de información que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad del usuario evitar en todo momento la fuga de la información del CDA que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Diariamente se almacenan copias de respaldo o backup de toda la información de la revisión técnico mecánica y de la operación de la prestación del servicio del CDA. Mensualmente se realizan dos copias en DVD, las cuales son entregadas así: Una al Gerente para que sea almacenada fuera de las instalaciones y otra en la oficina del ingeniero. Para asegurar que todo se pueda recuperar tras un desastre o fallo de los soportes.

4.3 Protección y ubicación de los equipos

Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Gerencia

General, en caso de requerir este servicio deberá solicitarlo al Director Técnico.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones del CDA.

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso.

Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro identificada como “datos” o similares, ya que las otras están destinadas para archivos de programa y sistema operativo.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos

Se debe evitar colocar objetos encima del equipo o cubrirlos orificios de ventilación del monitor o de la CPU.

Se debe mantener el equipo informático en un entorno limpio y sin humedad

El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

Queda prohibido que el usuario abra o desarme los equipos de cómputo.

4.4 Mantenimiento de equipos

Únicamente el personal autorizado por la Gerencia General o el Director Técnico de mantenimiento, podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo, cuando se demuestre negligencia por parte del usuario.

El resguardo para los computadores portátiles, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

El usuario deberá dar aviso inmediato a la Gerencia General, la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

4.5 Uso de dispositivos especiales

El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software que esté bajo contrato de licencia en el CDA y para respaldos de información que por su volumen así lo justifiquen.

La asignación de este tipo de equipo será previa justificación por escrito y autorización del Gerente General.

El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

Queda prohibido el uso de módems externos en las computadoras de escritorio.

Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el Gerente.

Los módems internos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones del CDA para conectarse a ningún servicio de información externo.

4.6 Daño del equipo.

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo u accesorio afectado. Para tal caso el Técnico de Soporte tendrá bajo su responsabilidad investigarlas causas y presentar el reporte correspondiente.

5. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

5.1 Política

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura tecnológica del CDA.
De igual forma , deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del CDA o hacia redes externas como Internet.

5.2 Uso de medios de almacenamiento

Toda solicitud para utilizar un medio de almacenamiento de información compartido deberá contar con la autorización de la gerencia.

El personal que requiera estos medios debe justificar su utilización. Dicha justificación deberá de presentarla a la Gerencia.

Los usuarios deberán respaldar diariamente la información sensitiva y crítica que se encuentre en sus computadoras personales o estaciones de trabajo.

En caso de que por el volumen de información se requiera algún respaldo en CD, este servicio deberá solicitarse al Director Técnico.

Los usuarios de informática del CDA deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial

Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información del CDA son registradas y susceptibles de auditoría.

5.3 Instalación de software.

Los usuarios que requieran la instalación de software que no sea propiedad del CDA, deberán justificar su uso y solicitar su autorización a la Gerencia General mediante solicitud escrita a través de un oficio firmado por el Director Técnico, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación

Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras estaciones de trabajo, servidores, o cualquier equipo conectado a la red del CDA, que no esté autorizado por la Gerencia General del CDA.

El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a la Gerencia General lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar al Director Técnico.

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del CDA debe ser reportado al Director Técnico y/o la Gerencia General.

5.4. Administración de la configuración

Los usuarios de las áreas del CDA no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos, u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del CDA, sin la autorización de la Gerencia y con el Vo.Bo del Director Técnico.

5.5. Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Gerencia General, en la cual los usuarios realicen la exploración de los recursos informáticos en la red del CDA, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad

5.6 Uso del correo electrónico

Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones)el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al CDA, a menos que cuente con la autorización de la Gerencia General.

Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del CDA.

Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del CDA.

Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones

El CDA se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violando políticas de Seguridad Informática CDA o realizado acciones no autorizadas.

El usuario debe de utilizar el correo electrónico del CDA única y exclusivamente a los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo quedando prohibido cualquier otro uso.

La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito al área de Atención a Usuarios, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Director General del área que corresponda.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

5.7 Controles contra código malicioso

Para prevenir infecciones por virus informático, los usuarios del CDA no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Empresa.

Los usuarios del CDA deben verificar la información y los medios de almacenamiento, considerando al menos discos flexibles, CD, cintas y cartuchos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el CDA.

Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser des comprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse

Ningún usuario del CDA debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas del CDA. El incumplimiento de este estándar será considerado una falta grave.

Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Gerencia.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Director Técnico de Soporte para la detección y eliminación del virus.

Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar al Director Técnico periódicamente las actualizaciones del software antivirus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el CDA en: Antivirus, Outlook, office, Navegadores u otros programas.

Debido a que algunos virus son extremadamente complejos, ningún usuario del CDA debe intentar erradicar los de las computadoras.

5.8 Internet

El acceso a Internet provisto a los usuarios del CDA es exclusivamente para las actividades

relacionadas con las necesidades del puesto y función que desempeña.

La asignación del servicio de Internet, deberá solicitarse por escrito a la Gerencia General, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Director Técnico.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el CDA, en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por la Dirección General de Informática.

Los usuarios de Internet del centro de CDA tienen que reportar todos los incidentes de seguridad informática al Director Técnico y/o a la Gerencia inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

Serán sujetos de monitoreo de las actividades que realiza en Internet.
•Saben que existe la prohibición al acceso de páginas no autorizadas.
•Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
•Saben que existe la prohibición de descarga de software sin la autorización de la Gerencia.
•La utilización de Internet es para el desempeño de su función y puesto en el CDA y no para propósitos personales.

6. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

6.1 Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y password necesarios para acceder a la información y a la infraestructura tecnológica del CDA, por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica del CDA, debe ser proporcionado por el dueño de la información, con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

6.2 Controles de acceso lógico.

El acceso a la infraestructura tecnológica del CDA para personal externo debe ser autorizado por la Gerencia del CDA, quien deberá notificarlo a la Dirección General de Informática quien lo habilitará.

Está prohibido que los usuarios utilicen la infraestructura tecnológica del CDA para obtener

acceso no autorizado a la información u otros sistemas de información de la Empresa.

Todos los usuarios de servicios de información son responsables por el User IDy password que recibe para el uso y acceso de los recursos

Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Gerencia General antes de poder usar la infraestructura tecnológica del CDA

Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del CDA, a menos que se tenga la autorización del dueño de la información y de la Gerencia General.

Cada usuario que acceda a la infraestructura tecnológica del CDA debe contar con un identificador de usuario (UserID) único y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios

Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (UserID).Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tienen prohibido utilizar el UserID de otros usuarios.

6.3. Administración de privilegios.

Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del CDA, deberán ser notificados al Técnico de Soporte con el visto bueno del Jefe del área.

6.4. Equipo desatendido.

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como passwords y protectores de pantalla (screensaver) previamente instalados y autorizados por la Dirección General de Informática cuando no se encuentren en su lugar de trabajo.

6.5. Administración y uso de Passwords

La asignación del password debe ser realizada de forma individual, por lo que el uso de passwords compartidos está prohibido.

Cuando un usuario olvide, bloquee o extravíe su password, deberá levantar un reporte a la Gerencia para que se le proporcione un nuevo password y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.

Está prohibido que los passwords se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

Sin importar las circunstancias, los passwords nunca se deben compartir o revelar. Hacer esto

responsabiliza al usuario que prestó su password de todas las acciones que se realicenconelmismo.

Todos, los usuarios, deberán observar los siguientes lineamientos para la construcción de sus passwords:

Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10), estos caracteres deben ser alfanuméricos.

Deben ser difícil es de adivinar, esto implica que los passwords no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y caracteres de control.

• No deben ser idénticos o similares a passwords que hayan usado previamente.

El password tendrá una vigencia de 90 días, finalizando este periodo el usuario recibe una solicitud electrónica de cambio de contraseña.

Todo usuario que tenga la sospecha de que su password es conocido por otra persona, deberá cambiarlo inmediatamente.

Los usuarios no deben almacenar los passwords en ningún programa o sistema que proporcione esta facilidad.

Los cambios o desbloqueo de passwords solicitados por el usuario al Centro de Atención a Usuarios (CAU) serán notificados con posterioridad por correo electrónico al solicitante con copia al Director General correspondiente, de tal forma que se pueda detectar y reportar cualquier cambio no solicitado.

6.6 Control de accesos remotos

Está prohibido el acceso a redes externas, cualquier excepción deberá ser documentada y contar con el visto bueno de la Gerencia General.

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y de la Gerencia General.

7. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

7.1 Política

La Gerencia General tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

7.2 Derechos de propiedad intelectual

Está prohibido por las leyes de derechos de autor y por del CDA, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por del CDA.

Los sistemas desarrollados por personal interno o externo que controle la Dirección General de Informática son propiedad intelectual del CDA.

7.3 Revisiones del cumplimiento

La Gerencia General o su delegado realizarán acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios, de acuerdo a lo establecido en su programa anual de trabajo.

La Gerencia General podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso del os recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal.

Los dueños de los procesos establecidos en del CDA deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad. Para la validación del software se utilizara el formato **MPO-01-R-06-1,** el cual se ejecutara dos veces al año. De igual forma se controlara el almacenamiento de backups con el formato **MPO-01-R07-1.** Y el registro de cambio de contraseñas de acceso al software por parte de los inspectores en el formato **MPO-01-R-06-2.**

7.4 Violaciones de seguridad Informática

Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.

Está prohibido realizar pruebas a los controles de los diferentes elementos de Tecnología de Información. Ninguna persona puede probar o intentar comprometer los controles internos.

Ningún usuario del CDA debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Gerencia General.

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código(programa)conocidos como virus, gusanos ó caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del CDA.

Nota 1:

- Se tiene una copia de respaldo externa la cual se actualiza cada quince días.

- Se debe dejar en una bitácora semanal el registro del back up con la cantidad de espacio almacenado.

- Cada seis meses se hace comprobación del back up con el proveedor del software.