Contraloría General
Departamento del Cesar
Hacia un Control Oportuno de la mano del Ciudadano

POLÍTICAS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

CÉSAR CERCHIARO DE LA ROSA
Contralor General del Departamento del Cesar

PATRICIA ÁLVAREZ ORTEGA
Profesional Universitario
Especialista en Seguridad Informática

RONAL YESID ROMERO SANDOVAL
Auxiliar Administrativo
Especialista en Seguridad Informática

Valledupar
2017

TABLA DE CONTENIDO

INTRODUCCIÓN

La información es el elemento activo de mayor valor para una entidad, protocolos de seguridad y leyes de archivo se han implementado para salvaguardar la información contenida en papel; a lo largo de los avances tecnológicos la información ha migrado en gran medida del papel impreso a los dispositivos digitales como discos duros, memorias extraíbles, unidades de disco y almacenamiento en la nube.

El Estado, no ajeno a estos cambios, ha visto la necesidad de plantear reglas para la creación, tratamiento, duplicación, almacenamiento y verificación de la información digital, así como el uso adecuado de los medios de comunicación que ofrecen las entidades para el desarrollo de las funciones de cada empleado.

La Contraloría General del Departamento del Cesar, como entidad pública del estado, presenta sus políticas de tecnologías de la información y la comunicación, para el tratamiento de las comunicaciones y la información que genera.

1. OBJETIVOS

- Implementar una gestión de manejo de los medios de comunicación, equipos de cómputo, tratamiento de información digital y demás sistemas electrónicos de uso institucional.

- Establecer disposiciones que garanticen el adecuado uso del software insertado en los equipos institucionales.

2. ALCANCE

Dando alcance a las políticas de ciber seguridad del Gobierno Nacional, en cabeza del Ministerio de Tecnologías de la Información y las Comunicaciones, enmarcado en el mejoramiento continuo de las tecnologías, con el fin de satisfacer las necesidades actuales y futuras de la estrategia laboral de la entidad, es necesario establecer criterios de innovación, calidad, eficiencia y escalabilidad, para así generar mejores resultados dentro del proceso misional.

Así mismo, establecer medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo o mal uso, que se pueda producir en forma intencional o accidental.

3. LINEAMIENTOS GENERALES

Responsabilidad: Es responsabilidad del Representante legal de la entidad, por medio del área de Sistemas, hacer uso de la política de TIC como parte de sus herramientas de gobierno, gestión y definición de estándares, procedimientos y lineamientos que garanticen su cumplimiento.

Cumplimiento: El cumplimiento de la Política de Tecnologías de la Información y Comunicación (TIC) es obligatorio. Si los Jefes de Oficina, funcionarios o terceras partes violan estas políticas, la Entidad se reserva el derecho a tomar las medidas correspondientes conforme a las normas y la Ley.

Excepciones: Las excepciones a cualquier cumplimiento de Política de Tecnologías de la Información y Comunicación (TIC), deben ser aprobadas por el área de Sistemas, previa autorización del representante legal de la entidad. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas por la oficina de Sistemas.

Administración de las Políticas: Las modificaciones o adiciones de la Política de Tecnologías de la Información y Comunicación (TIC), serán propuestas por el Comité Operativo de Sistemas y aprobadas por el Comité Administrativo de Sistemas. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

4. DEFINICIONES

Se definirán los siguientes conceptos:

- **Activo:** Cualquier elemento físico o digital que tenga valor para la Entidad.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la Entidad.
- **Arquitectura Empresarial:** Conjunto de elementos organizacionales (estrategia, estructura, procesos, tecnología, personas) que se relacionan entre sí, garantizando la alineación desde los niveles más altos (estratégicos), medios (tácticos), hasta los más bajos (operativos), con el fin de optimizar la generación de productos y servicios que conforman la propuesta de valor entregada al público.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Continuidad:** Capacidad de la Gestión de Servicios de Tecnología para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.

- **Desastre o contingencia:** Interrupción de la capacidad de acceso a información y procesamiento de la misma, por medio de equipos de cómputo u otros medios necesarios para la operación normal de un negocio.

- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de una persona o entidad autorizada.

- **Evaluación del Riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

- **Impacto:** La consecuencia que al interior de la entidad se produce al materializarse una amenaza.

- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos.

- **La Entidad:** Se refiere a la Contraloría General del Departamento del Cesar.

- **Operación:** Actividades diarias realizadas para soportar y entregar los servicios de tecnología.

- **Políticas:** Toda intención y directriz expresada formalmente por la administración de la Organización.

- **Procedimientos:** Pasos operacionales que los funcionarios deben realizar para alcanzar ciertos objetivos o resultados.

- **Procesos:** Se define proceso a un conjunto de actividades que reciben una o más entradas para crear un resultado o producto de valor para el cliente o para la propia entidad. Normalmente, una actividad empresarial cuenta con múltiples procesos que sirven para el desarrollo de su función Constitucional.

- **Representante Legal:** El Contralor General del Departamento del Cesar.

- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Puede involucrar otras propiedades como autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

- **TIC:** Se refiere a las Tecnologías de Información y Comunicación.

- **Vulnerabilidad:** Debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

5. POLÍTICA DE ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE LAS TIC

El Representante Legal, a través de la Oficina de Sistemas, es responsable de la adquisición, implementación y mantenimiento de todos los servicios y configuración de las Tecnologías de Información y Comunicación (TIC), buscando asegurar la calidad de los servicios entregados y de acuerdo con los criterios de innovación, confiabilidad, disponibilidad, seguridad, economía e interoperabilidad, dentro del marco legal.

6. ESTÁNDARES DE LA POLÍTICA DE ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE LAS TIC

- **Controles criptográficos:** La adquisición, instalación e implementación de controles criptográficos se realizan con base en una evaluación de riesgos que identifique el nivel de complejidad requerido, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido para las aplicaciones o procedimientos.

- **Desarrollo de aplicaciones:** Las aplicaciones que se desarrollen producto de convenios, contratos o por los funcionarios internos como apoyo a la gestión; deben cumplir con los requerimientos de seguridad establecidos por la Entidad, conforme con la Política de Seguridad de la Información, que se desarrolla más adelante en este documento.

- **Documentación:** La documentación de cada uno de los sistemas implantados en la Entidad, debe contener la guía para brindar soporte técnico y de usuario, la cual incluya copia del contrato con el proveedor que lo brinda (en caso de que aplique esta modalidad, especificando los Acuerdos de Nivel de Servicio Establecidos, los interlocutores y los procedimientos para obtener el servicio).

- **La Propiedad Intelectual:** Los desarrollos contratados o realizados por los funcionarios dentro de su trabajo será propiedad de la Entidad, salvo acuerdo escrito expreso que diga lo contrario, para los desarrollos en operaciones de convenios interadministrativos se realizará el formato de propiedad intelectual de común acuerdo y con base a los parámetros establecidos en el convenio.

- **Acceso a Sistemas:** Los funcionarios o terceros que tengan acceso a los sistemas TIC de la Entidad, no podrán copiar ni ceder, sin autorización, las

aplicaciones que son propiedad de la entidad, las de propiedad mixta por convenios, ni las aplicaciones o programas de los que esta tenga licencia de uso.

- **Control de Cambios:** Los procedimientos de control de cambios deben estar documentados y ser ejecutados bajo los controles adecuados a fin de no comprometer la seguridad de los sistemas.

- **Manejo de Aplicaciones:** Para el manejo y administración de las aplicaciones tecnológicas, los funcionarios dueños de los procesos en la entidad, tienen la responsabilidad de hacer las pruebas necesarias e informar a la Oficina de Sistemas los errores o solicitudes de mejoras.

- **Procesos de Desarrollo y Soporte:** El proceso de adquisición y desarrollo de las aplicaciones debe ser estructurado y ordenado, considerando las diferentes etapas del ciclo de vida de las soluciones informáticas.

- **Requerimientos Tecnológicos:** Cuando un área requiera implementar un software, plataforma tecnológica o sistemas de información, debe diligenciar el respectivo formato de requerimientos y asignar a una persona responsable para liderar la implementación solicitada.

- **Seguridad en los Archivos del Sistema:** El acceso a los archivos del sistema y al código fuente debe ser restringido. La actualización del software, aplicativos y las librerías solo pueden ser manipuladas por el líder de la Oficina de Sistemas o un tercero (contratista o funcionario de convenio) bajo autorización del representante legal, considerando que para el software de proveedores, las actualizaciones y migración a nuevas versiones se deben realizar antes de que termine la vigencia del soporte.

- **Responsabilidades para la Seguridad de la Información:** La Contraloría General del Departamento del Cesar, es el propietario de la información. Por ello todos los funcionarios deben ser conscientes de los riesgos a la que está expuesta la información a su cargo, de forma que ejerzan frente a sus colaboradores el liderazgo apropiado para disminuirlos.

- **Revisión Independiente en Seguridad de la Información:** La Oficina de Control Interno, debe implementar y ejecutar un plan de auditoría de seguridad de la información. Este plan debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad. Los resultados deben generar un programa de seguridad, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables. El programa debe ser aprobado por el Comité Administrativo de Sistemas.

- **Seguridad en los Accesos por Terceros:** La Oficina de Sistemas debe realizar una evaluación para identificar el riesgo de acceso por terceros a la información de la Entidad.

7. INFRAESTRUCTURA INFORMÁTICA

Responsabilidades de la operación: Los procedimientos de operación deben considerar la planeación de la operación, el tratamiento y manipulación de la información, las copias de respaldo, el manejo de errores o excepciones durante la ejecución de un trabajo, los contactos de apoyo para el caso de dificultades operacionales o técnicas inesperadas, reinicio de los sistemas y procedimientos de recuperación a utilizar en caso de falla del sistema, gestión de pistas de auditoría y sistemas de registro de información, y el aseguramiento de plataformas.

Separación de Ambientes: Para minimizar los riesgos en el proceso de puesta en producción de los cambios y nuevos desarrollos de software, así como el impacto por la no disponibilidad de los servicios, se debe establecer una segregación de ambientes, (Desarrollo, Pruebas y Producción), considerando:

- Definir y documentar las reglas para el paso de software entre ambientes.
- El uso de diferentes equipos, dominios y directorios.
- La restricción de uso de compiladores, editores y otras herramientas de desarrollo o recursos del sistema en ambientes de producción.
- Los sistemas de prueba deben emular al sistema productivo tan real como sea posible.
- El uso de perfiles de usuario diferentes para los diferentes ambientes.
- Los menús deben mostrar mensajes de identificación adecuados para reducir el riesgo de error.
- La restricción de uso de datos de producción en ambientes de prueba. En caso de ser necesario se debe utilizar un mecanismo de enmascaramiento.

Planificación y Aceptación: Se deben establecer proyecciones de capacidad futura, para reducir el riesgo de sobrecarga del sistema.

Se hará monitoreo al uso de los servicios de red y de los sistemas, con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño requerido para cumplir con los Acuerdos de Niveles de Servicio y reducir el riesgo de posibles fallas.

Protección Contra Códigos Maliciosos: Se deben implementar controles de detección, prevención, recuperación y concientización, con el fin de que los usuarios tengan protección frente a códigos maliciosos.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y acorde con la propiedad intelectual.

Gestión de Seguridad en las Redes: Las redes y la infraestructura de apoyo deben ser adecuadamente gestionadas y aseguradas para protegerlas de amenazas y para mantener la seguridad de los sistemas y aplicaciones.

Se deben implantar controles relacionados con la segmentación, gestión, monitoreo y detección de eventos, para asegurar la información que viaja por las redes.

Manejo de los Medios Magnéticos: Establecer procedimientos adecuados para proteger los medios magnéticos de respaldo, esto para prevenir la revelación, modificación, eliminación o destrucción no autorizada.

Todo medio magnético utilizado que no se requiera, debe ser destruido, de manera que no se pueda recuperar la información. En el caso de documentos, estos se deben destruir con las herramientas adecuadas.

Debe existir un inventario de medios magnéticos y deben almacenarse de acuerdo con las prescripciones del fabricante para prevenir la pérdida o deterioro de la información; igualmente, todos los medios deben ser etiquetados de acuerdo con el procedimiento de clasificación y manejo de la información establecido por la Entidad.

Los medios se deben de proteger contra el acceso no autorizado, el mal uso o corrupción, dentro y fuera de los límites físicos de la Entidad (Si es del caso).

Registros de Auditoría: Se deben conservar registros de la información sensible de los equipos informáticos de los funcionarios (incluyendo directivos).

8. TELECOMUNICACIONES

Uso de las Redes: El líder de la Oficina de Sistemas, es el responsable de definir las necesidades que tiene la compañía con respecto a las redes. Es responsable también de la administración de los anchos de banda necesarios para soportar los servicios TIC.

El uso de las redes será monitoreado con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño requerido para cumplir con los Acuerdos de Niveles de Servicio y reducir el riesgo de posibles fallas.

Telefonía fija: La asignación de extensiones telefónicas y modificación de los planes de acceso, se harán de acuerdo con las necesidades descritas en el formato diligenciado de solicitud, el cual debe ser entregado al líder de la Oficina de Sistemas, con el fin de ser evaluado por el comité operativo y aprobado por el comité administrativo de

sistemas; después de ser aprobados, se iniciará comunicación con el proveedor de outsourcing de telecomunicaciones.

El uso de los teléfonos fijos asignados a los funcionarios debe ceñirse al desarrollo de actividades relacionadas con el cargo y los objetivos misionales de la entidad.

9. POLÍTICA DE USO PARA EQUIPOS DE CÓMPUTO DE ESCRITORIO, PORTÁTILES Y DISPOSITIVOS MÓVILES

La Entidad, por medio de la Oficina de Sistemas, establece los requisitos y controles para la conexión de equipos de cómputo, portátiles y los dispositivos móviles a la red de la compañía.

Los funcionarios, consultores, contratistas y terceras partes, podrán hacer uso de los dispositivos móviles, siempre y cuando cumplan con los criterios técnicos, funcionales, de seguridad, regulatorios y económicos establecidos por la Entidad.

9.1. Del Uso de los Equipos de Cómputo de Escritorio y Portátiles

Todo funcionario, consultor, contratista y/o tercera parte, tiene el derecho laboral de utilizar un equipo de cómputo para el desarrollo de sus actividades, si la Entidad le provee uno, este debe cumplir con la verificación y visto bueno de su funcionamiento por parte de la Oficina de Sistemas, estos equipos cuentan con las licencias necesarias y está prohibido realizar cualquier instalación, modificación o eliminación de aplicaciones en los equipos sin el adecuado consentimiento de la Oficina de Sistemas.

Si la persona desea ingresar un equipo de cómputo o dispositivo móvil personal, este deberá ser verificado por la Oficina de Sistemas, con el fin de dar cumplimiento a la revisión de parámetros mínimos para la conexión de equipos en la red de datos. El uso que se le dé al equipo de cómputo personal, es decisión del dueño, pero el uso de la red de datos (Internet) está sujeta a las prohibiciones propias de la Entidad.

9.2. Del Uso Adecuado de la Red de Datos (Internet)

Todo equipo conectado a la red de la Entidad deberá tener actualizadas todas sus aplicaciones, sistema operativo y antivirus; igualmente se deberá contar con la autorización previa de la oficina de sistemas para poder acceder a la red de datos local (LAN) y la red externa (WAN).

La Oficina de Sistemas es la responsable del monitoreo de la red y verificación del cumplimiento de los estándares de conexión. Ningún funcionario, consultor, contratista o tercera parte está autorizado para suministrar datos de conexión a la red de la

Entidad, sin el conocimiento de la Oficina de Sistemas, previa verificación del cumplimiento de los requisitos.

Una vez el equipo de cómputo de escritorio, portátil o dispositivo móvil se encuentre en la red, es perentorio informar que está prohibida la utilización de esta para acceder a contenido ilegal como:

- Contenido sexual para adultos
- Contenido sobre compra o distribución de drogas ilícitas y sustancias psicoactivas
- Contenido de connotación terrorista
- Contenido de agresiones físicas o psicológicas
- Contenido de juegos de azar

El uso de la red de datos estará supeditada a las necesidades propias del desarrollo del trabajo de cada funcionario; si esto no se cumple es obligación de la Oficina de Sistemas realizar el reporte correspondiente e informe a la dirección.

10. POLÍTICA DE SOPORTE A LOS USUARIOS DE LAS TIC

La Oficina de Sistemas, será el único canal por medio del cual se reportará cualquier incidente o requerimiento asociado a las TIC, con el fin de garantizar el seguimiento y entrega oportuna del servicio solicitado.

11. POLÍTICA DE RELACIÓN CON INFRAESTRUCTURA DE TERCEROS

La infraestructura tecnológica de la Entidad que se expone a terceros, debe ser siempre evaluada y aprobada por el Comité Operativo de Sistemas TIC, esto con el fin de lograr una sola vía de comunicación y actualización de la infraestructura de la Entidad.

12. POLÍTICA DE GESTIÓN DEL RIESGO TIC

El Comité Operativo de Sistemas TIC debe identificar, calificar, priorizar y realizar el tratamiento de los riesgos tecnológicos, con base en los objetivos del Plan de Acción y de acuerdo con la Política de gestión de riesgos de la entidad, este informe debe ser presentado al Comité Administrativo de Sistemas TIC.

13. POLÍTICA DE INCORPORACIÓN AL CUMPLIMIENTO REGULATORIO

Toda solución de servicios o infraestructura tecnológica debe cumplir con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la Entidad.

14. POLÍTICA DE PROTECCIÓN DEL MEDIOAMBIENTE

El desarrollo de las TIC debe orientarse bajo las estrategias globales de protección del medioambiente y de la Política del Sistema de mejoramiento de la calidad y gestión medioambiental de la entidad, para reducir el impacto medio ambiental.

15. POLÍTICA DE MANEJO Y PROTECCIÓN DE LA INFORMACIÓN

Todos los funcionarios, consultores, contratistas y terceras partes que manejen información de la empresa, están obligados a salvaguardarla en los sitios dispuestos para tal fin, para garantizar la disponibilidad, confidencialidad y respaldo de la misma.

15.1. Estándares de la Política de manejo y protección de la información

Carpetas compartidas: El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información. Por lo tanto, su uso debe ser controlado y para eso se debe evitar el uso de carpetas compartidas en equipos de escritorio; en los casos que sea necesario se deberá solicitar permiso escrito a la Oficina de Sistemas, quien será la encargada de configurar la carpeta y sus niveles de seguridad.

El usuario que autoriza el acceso a las carpetas y dispone el recurso compartido, es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

Se debe definir el tipo de acceso y los roles estrictamente necesario sobre la carpeta (lectura, escritura, modificación, borrado). Además, se debe especificar el límite de tiempo durante el cual estará publicada la información y el recurso compartido en el equipo.

El acceso a carpetas compartidas debe delimitarse a los usuarios que realmente necesitan la información y se debe proteger el ingreso con contraseñas.

No se puede compartir carpetas o el acceso a carpetas compartidas, a usuarios que no cuenten con software de antivirus corporativo y actualizado.

Respaldo de la información: Con el fin de mantener un respaldo de los datos críticos de información de la Entidad, la Contraloría General del Departamento del Cesar mantendrá activo los siguientes protocolos:

- **Equipos de Cómputo Funcionarios:** Se debe realizar un respaldo (Backup) de la información sensible de los discos duros de cada computador, mínimo una vez cada dos años o cuando el funcionario salga de la entidad; estos respaldos se deben mantener durante un período no menor a tres años, con el fin de ayudar en investigaciones futuras y en el seguimiento y monitoreo del control de acceso.

  En la medida de lo posible se incluirá como mínimo en los registros:

  - Identificadores de usuarios.
  - Registro de intentos de acceso al sistema exitoso y rechazado.
  - Cambios en la configuración del sistema.
  - Uso de privilegios.
  - Uso de dispositivos y aplicaciones del sistema.
  - Cambios o intentos de cambios en las posiciones y en los controles de seguridad del sistema.

- **Servidor de Datos:** El servidor de datos de la entidad se debe configurar para generar un respaldo (Backup) diario de los datos críticos de su sistema e información de las aplicaciones; adicionalmente, se realizará un respaldo en por medio de una unidad magnética externa semanalmente, la cual se mantendrá asegurada por parte de la Oficina de Sistemas.

- **Página Web:** El respaldo de seguridad de la información perteneciente a la página web institucional, se realizará semanalmente por parte de la Oficina de Sistemas, realizando copia magnética en unidad extraíble.

Las copias de seguridad de la información y de software se deben realizar periódicamente, considerando lo siguiente:

- Establecer registros precisos y completos de las copias de seguridad y procedimientos de recuperación documentados.
- La extensión y frecuencia de las copias de seguridad (totales o incrementales) debe supeditarse a los requisitos de negocio, legales y de seguridad, respecto a la criticidad de la información.
- Las copias de seguridad deben almacenarse en un lugar diferente al de la ubicación principal.
- La retención de las copias de seguridad será acorde con las tablas de retención definidas en el Sistema de Gestión Documental o en el Sistema de Gestión de Calidad.

Responsabilidad de uso: La Entidad pone al servicio de los funcionarios el uso de los medios necesarios para el normal desarrollo de las labores propias del cargo, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta. Es deber de los funcionarios acogerlas con integridad y dar a los recursos uso racional y eficiente.

La Entidad, en respeto de los principios de libertad de expresión y privacidad de información, no genera a los funcionarios ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medios electrónicos que sean propiedad de la Entidad. En consecuencia, podrá denegar el acceso a los servicios electrónicos, inspeccionar, monitorear y cancelar servicios asignados como correo electrónico, navegación en Internet y recursos compartidos, entre otros.

Los usuarios de los servicios electrónicos aceptan y convienen que la Entidad puede conservar y revelar el contenido del correo si así le es requerido por Ley y un Juez de la República o si el funcionario, de buena fe y presentando aceptación firmada y autenticada, considera que dicha reserva o revelación es necesaria para: (a) cumplir con procesos legales, (b) responder a quejas de que algún contenido viola los derechos de terceras personas, o (c) proteger los derechos, propiedad o seguridad personal de la Entidad, sus usuarios y el público en general.

La violación de los controles de seguridad o el incumplimiento de las Políticas de la Entidad por parte de los funcionarios dará lugar a la aplicación de medidas administrativas, disciplinarias, civiles o penales a las que haya lugar.

16. USO DE LOS SISTEMAS Y EQUIPOS DE CÓMPUTO.

La Entidad tiene regla de renuncia (disclaimer) que debe utilizarse al inicio de sesión en los equipos de cómputo:

"¡Advertencia! Este sistema (hardware, software y periféricos), así como la información en él contenida es propiedad de la Contraloría General del Departamento del Cesar y su uso está restringido únicamente para propósitos de la Contraloría General del Departamento del Cesar, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de este sistema implica su consentimiento con esta política."

17. POLÍTICAS DEL USO DE CORREO ELECTRÓNICO

- La Entidad, como muestra del respeto por los principios de libertad de expresión y privacidad de información, no generará en los funcionarios, colaboradores o

terceras personas que posean por autorización de la Oficina de Sistemas una cuenta de correo electrónico, ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medio del sistema de correo electrónico propiedad de la Entidad; en consecuencia, podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado.

- Las comunicaciones por correo electrónico entre la Entidad y su público de interés, deben hacerse a través del correo homologado y proporcionado por la empresa. No es permitido utilizar cuentas personales para comunicarse con el público de interés de la Entidad, ni para transmitir cualquier otro tipo de información misional.

- A los colaboradores, que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna en el servidor una vez son vinculados. La Secretaría General por medio del Profesional de Talento Humano, es responsable de informar a la Oficina de Sistemas, las vinculaciones que requieran creación de cuentas de correo; de igual manera debe informar oportunamente los retiros de funcionarios y colaboradores para la suspensión de este servicio, mediante el respectivo formulario diligenciado.

- Esta cuenta estará activa durante el tiempo que dure la vinculación del colaborador con la Entidad, excepto en casos de fuerza mayor o mala utilización que eventualmente puedan causar la suspensión o cancelación de la misma. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor mediante una solicitud enviada a la Oficina de Sistemas.

- La capacidad máxima para almacenamiento de correo electrónico está definida por la Oficina de Sistemas. No obstante, en caso de necesidades especiales, el interesado podrá solicitar la ampliación de la capacidad o uso. De igual manera, en caso de necesidad (por razones de sus funciones), las capacidades máximas de los buzones podrán ser modificadas unilateralmente por parte de la Entidad.

- La Entidad tiene regla de renuncia (disclaimer) que debe utilizarse siempre en los mensajes. Para evitar reclamaciones legales todos los usuarios de correo de la Entidad tienen que hacer pública la renuncia de responsabilidad legal por el envío de la información. El disclaimer aprobado es:

  "La información contenida en este mensaje y en sus anexos es estrictamente confidencial. Si usted recibió por error esta comunicación, por favor notificar inmediatamente esta circunstancia mediante reenvío a la dirección electrónica del remitente y bórrela puesto que su uso no autorizado acarreará las sanciones y medidas legales a que haya lugar. La Entidad no se hace responsable por la presencia en este mensaje o en sus anexos, de algún virus o malware que pueda generar o genere daños en sus equipos, programas o afecte su información".

"The information contained in this message and its attachments is strictly confidential. If you received this communication in error, please immediately notify the sender of the situation by replying it to sender email address and delete this message as its unauthorized use shall derive in applicable penalties and legal actions. The Company is not liable for the presence of any virus or malware in this message or its attachments that cause or may cause damage to your equipment, software or that affects your information."

- El buzón de correo es personal e intransferible y corresponde al funcionario o colaborador velar por la seguridad, protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia, al aceptar el buzón otorgado por la Entidad, el usuario se compromete a:

  - Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.

  - El funcionario o colaborador titular de correo o cuenta asignada por la organización, usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores propias de su cargo o de las investigaciones que tenga asignadas; las únicas áreas autorizadas para el envío de correos masivos son el Despacho, la Oficina de Sistemas y la Ventanilla Única. Otras necesidades de comunicación masiva deben ser aprobadas por la Oficina de Sistemas.

  - El uso del correo electrónico propiedad de la Entidad, deberá ser usado solamente para fines misionales. En su uso el funcionario o colaborador actuará siempre con respeto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofendan la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros (Excepto las autorizadas por la Oficina de Sistemas, previo consentimiento del Representante Legal.

  - La Entidad se abstiene de enviar o recibir los mensajes de sus usuarios con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contengan difusión de noticias sin identificar plenamente su autor; adicionalmente, los funcionarios y colaboradores no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualesquiera que contenga mensajes duplicativos o no solicitados, u otra información ajena a las labores que desempeñan en su cargo.

- Los funcionarios y colaboradores de la Entidad se abstendrán de utilizar la cuenta para el envío o reenvío de mensajes Spam (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), Hoax (es un intento de hacer creer que algo falso es real, con la intención de llamar la atención del lector y hacerlo caer en estafas o infecciones del equipo), con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus, malware, alcohol, drogas ilícitas o pornografía), o que sea contrario a las políticas y normas institucionales.

- Evitar el envío desde su buzón de elementos (textos, software, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En especial, es necesario evitar la distribución de software que requiera licencia, claves ilegales de software, programas para romper licencias (crackers), y en general, cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario, con perjuicio de las responsabilidades que eventualmente puedan surgir ante la Ley.

- Realizar mantenimiento periódico de su correo, cuando el sistema le haga advertencias de espacio disponible. Estas advertencias se realizan varias veces, por lo que debe estar atento e informar a la Oficina de Sistemas, cuando requiera la depuración del mismo.

- Utilizar la cuenta de correo electrónico de la Entidad para fines laborales, de investigación y los estrictamente relacionados con las actividades propias de su trabajo. Los colaboradores deben evitar usar el buzón de correo electrónico para fines comerciales diferentes a los que sean relativos al interés de la Entidad.

- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red de la Entidad.

- Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente haya sido dirigido a un grupo grande de usuarios; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.

- Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas (Podría tratarse de un virus o

malware). En particular, no abrir mensajes cuyo asunto contenga palabras en inglés a menos que lo esté esperando.

- En lo posible, es necesario evitar usar letras mayúsculas, especialmente en el campo de "Asunto:", al igual que el uso excesivo de signos de exclamación (&, %, $, #, ?, ¡, !, ¿), esto puede hacer que los sistemas de correo lo identifiquen como correo no deseado (Spam), y el mensaje posiblemente no llegue al destinatario, o llegue con identificación de correo no solicitado.

18. NAVEGACIÓN EN INTERNET

El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la Entidad y deben ser utilizados por los funcionarios y colaboradores para realizar las funciones establecidas para su cargo, por lo cual la Entidad definió los siguientes parámetros para su uso:

- El funcionario o colaborador debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.

- La descarga de música y videos no es una práctica permitida.

- Evitar el uso de servicios descarga de archivos como: jdownloader, utorren, KaZaA, Emule, LimeWire, Morpheus, GNUtella o similares.

- Abstenerse de usar sitios que salten la seguridad del servidor de acceso a Internet (proxy).

- El uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral y que dio origen a la habilitación del servicio, no está permitido.

- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los funcionarios y colaboradores de la Entidad; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.

- Los funcionarios y colaboradores no deberán coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos de la entidad o cualquier otro derecho intelectual de otra persona.

- Abstenerse de coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que viole la Ley o de la cual puedan surgir responsabilidades u obligaciones de carácter criminal o civil bajo cualquier Ley estatal, local, nacional o internacional; incluyendo, pero no limitado, las Leyes y regulaciones de control y exportación de Colombia y de los decretos sobre fraudes de computación.

- Coleccionar, almacenar, divulgar, transmitir o solicitar información personal (incluyendo sin limitación alguna, información biográfica, habitacional, social, marital, ocupacional, financiera y de salud) sobre otros usuarios, sin su consentimiento o conocimiento, son prácticas no permitidas por la Entidad.

- Los funcionarios y colaboradores se deben abstener de coleccionar, divulgar, transmitir o solicitar programas de computación dañinos, virus, códigos, expedientes o programas.

- Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "las pirámides", son faltas se constituyen como violaciones a esta Política.

- No está permitido personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal.

- Hacer o intentar hacer, cualquier cosa que afecte desfavorablemente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios", ataques contra otros sistemas o contra el anfitrión de redes u otros usuarios, se constituye como una violación a esta Política.

19. USO DE HERRAMIENTAS QUE COMPROMETEN LA SEGURIDAD

Hacer o intentar hacer, sin permiso del dueño o del anfitrión del sistema o de la Oficina de Sistemas, cualquiera de los siguientes actos:

- Acceder el sistema o red.
- Monitorear datos o tráfico.
- Sondear, copiar, probar firewalls o herramientas de hacking.
- Atentar contra la vulnerabilidad del sistema o redes.
- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

20. COMPUTACIÓN EN NUBE

Ninguna información de la Contraloría General del Departamento Del Cesar, podrá utilizar tecnologías de computación en nube si no está previamente autorizado por la Oficina de Sistemas, previo visto bueno del representante legal.

21. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Se deben establecer responsabilidades y procedimientos para tratar los eventos y los puntos débiles de seguridad de la información de forma efectiva. Una vez que se hayan comunicado a través de un proceso de mejora continua, la Oficina de Sistemas se encargará de analizar la causa y evaluar conforme al proceso de gestión de problemas.

Cuando se detecta por primera vez un evento de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro que se destruyan de forma intencional o accidental de las pruebas necesarias antes de tomar conciencia de la gravedad del incidente. Por lo cual, frente a cada evento de seguridad de la información, se debe efectuar reunión del Comité Administrativo de Sistemas, para evaluar cualquier acción legal que se esté considerando, así como asesorarse de las pruebas necesarias.

Cuando una acción contra un funcionario o la Entidad, después de un incidente de seguridad de la información, implique medidas legales (tanto civiles como penales), deberán recopilarse pruebas, que deberán conservarse y presentarse de manera que se ajusten a las normas legales vigentes.

A la hora de la recopilación de las pruebas, se preservará la cadena de custodia y se utilizarán herramientas y procedimientos aceptados de análisis forenses.

22. REFERENCIAS

- Constitución Política de Colombia. 1991.
- Ley 1273 de 2009
- Manual de la Política De Seguridad para las Tecnologías de la Información y las Comunicaciones – TICS. Presidencia de la República (http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Sistema-Seguridad-Informacion.pdf)
- Política Seguridad de la Información. CELSIA

(http://www.celsia.com/Portals/0/contenidos-celsia/nuestra-empresa/politicas-y-adhesiones/politicas/politica-seguridad-de-la-informacion.pdf)

- Política de Seguridad de la Información. INVIMA (https://www.invima.gov.co/images/stories/formatotramite/GDIDIEPL010version2.pdf)

CÉSAR CERCHIARO DE LA ROSA
Contralor General del Departamento del Cesar

Proyectó: Ronal Yesid Romero Sandoval
Auxiliar Administrativo

Revisó: Patricia Álvarez Ortega
Profesional Universitaria

Aprobó: Diana Orozco Sánchez
Contralora Auxiliar