	Resolución: 003471 Fecha: 03 SEP 2019
	Por la cual se regulan las Políticas de Seguridad y Privacidad de la información del Departamento del Cesar

EL GOBERNADOR DEL DEPARTAMENTO DEL CESAR

En ejercicio de las facultades conferidas en los artículos 61, 209 y 305 de la Constitución Política emanado de la Presidencia de la Republica y

CONSIDERANDO

Que el Decreto 1008 del 14 de Junio de 2018 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital en su Artículo 2.2.9.1.1.3. **Principios**, dispone que la Política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998, 3° de la Ley 1437 de 2011, 2° y 3° de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2° de la Ley 1341 de 2009.

Que Artículo 2.2.9.1.3.3. de la misma norma, **Responsable de orientar la implementación de la Política de Gobierno Digital** establece "*Los Comités Institucionales de Gestión y Desempeño de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015, serán los responsables de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión*".

Que igualmente en el parágrafo 2° del Artículo 2.2.9.1.4.1. del mismo decreto, **Seguimiento y Evaluación**, señala "*El seguimiento y la evaluación del avance de la Política de Gobierno Digital se realizará con un enfoque de mejoramiento continuo, verificando que cada sujeto obligado presente resultados anuales mejores que en la vigencia anterior, de acuerdo con la segmentación de entidades definida en el artículo 2.2.9.1.4.2 del presente Decreto*".

Que se hace necesario establecer la Política de Seguridad y Privacidad de la Información como herramienta que permita mitigar, eliminar o trasladar el riesgo de seguridad de información del Departamento del Cesar.

Que el Departamento del Cesar cuenta con una serie de recursos tecnológicos vitales para el desarrollo de las actividades de carácter misional y administrativo, por tal motivo es importante reconocer los riesgos que implica el uso de este tipo de herramientas y las condiciones ideales que optimizan su productividad, para tales fines es fundamental el desarrollo de políticas de seguridad y privacidad de información que apoyen los esfuerzos técnicos y que apunten a un modelo sostenible, productivo, progresivo y altamente adaptable a los ritmos acelerados de la tecnología.

En virtud de lo anterior

RESUELVE

CAPITULO I
Aspectos Generales

Artículo 1. Objeto: La presente resolución tiene por objeto establecer las políticas de seguridad y privacidad de la información del Departamento del Cesar, garantizando la confidencialidad, integridad y disponibilidad de la misma, buscando mitigar, eliminar o trasladar el riesgo de seguridad de información, con el fin de lograr el cumplimiento de las metas y objetivos propuestos.

Artículo 2. Ámbito de Aplicación: La presente resolución aplica a todos los funcionarios, contratistas y terceros del Departamento del Cesar.

CAPITULO II
Directrices establecidas por la dirección para la seguridad de la información

Artículo 3. Alta Dirección: El Departamento del Cesar a través de la Alta Dirección manifiesta su apoyo y compromiso en el desarrollo y puesta en marcha de la Política de Seguridad y Privacidad de la Información de la entidad, asignando los recursos necesarios que permitan alcanzar los objetivos planteados en la misma.

Artículo 4. Gobierno Digital: En cumplimiento de las políticas establecidas por gobierno digital, se fortalecen las actividades desarrolladas en la implementación del Modelo de Seguridad y Privacidad de la Información que establece el Departamento Cesar, se elaboran una serie de políticas que se describen a continuación:

a) La entidad, en cumplimiento de la política de gobierno digital, considera de vital importancia la implementación y adopción la Política de Seguridad y Privacidad de la Información, para el desarrollo y buen funcionamiento de los procesos y procedimientos de la entidad.

b) El Departamento del Cesar define unos objetivos, orientados a reducir los niveles de riesgos dentro y fuera de la institución, objetivos que permiten mejorar la seguridad de información de la entidad, entendiéndose está como la preservación de la confidencialidad, integridad y disponibilidad de la información, aumentando la confianza en los servidores públicos, contratistas y terceros, todo lo anterior, es fortalecido mediante el cumplimiento de la política de seguridad y privacidad de la información.

c) El desarrollo, cumplimiento, comunicación, monitoreo y mantenimiento de la política de seguridad y privacidad de la información, enmarcado dentro del Modelo de Seguridad y privacidad de información, se realizará, con base a los resultados obtenidos, un proceso de mejoramiento continuo de análisis y valoración del riesgo de seguridad de información, donde surgirán las acciones a desarrollar, en materia de seguridad y privacidad de la información, dentro y fuera de la entidad, debidamente autorizado y divulgado por la Alta Gerencia del Departamento del Cesar.

d) La Alta Dirección de la entidad, con base en los criterios de evaluación del riesgo establecerá las acciones a seguir, de tal forma que permita minimizar los niveles de los mismos, y en ese sentido los riesgos sean tratados adecuadamente y mitigados. La Alta Dirección del Departamento del Cesar, desarrollará y pondrá en marcha un Plan de Continuidad del Negocio, acorde a las necesidades de la entidad, dimensionando los riesgos que le puedan afectar.

e) La Alta Dirección del Departamento del Cesar se compromete a la implementación, mantenimiento y mejora de la política de seguridad y privacidad de la información en el marco del Modelo de Seguridad y Privacidad de Información (MSPI) de la Estrategia de la política de Gobierno Digital, ofreciéndoles los medios y recursos que sean necesarios e invitando a todos los servidores públicos, contratistas y terceros, que adopten y cumplan la política de seguridad y privacidad de la información.

f) Para esto, el comité de gestión y desempeño del Departamento del Cesar aprobará las Políticas de Seguridad y Privacidad de la Información creando conciencia en todos los Servidores Públicos, Contratistas y Terceros, para que vean la política de seguridad y privacidad de información como los lineamientos que permiten mitigar los riesgos en materia de seguridad de la información.

g) La responsabilidad general de la seguridad y privacidad de información recae sobre la Alta Dirección de la entidad y el Profesional de Seguridad de la Información. Por otro lado, todos los funcionarios, Contratistas y terceros, tienen la obligación de reportar los

incidentes, en materia de seguridad de información, través del formato de reporte de incidentes.

h) Todo lo relacionado con la Política General de Seguridad y Privacidad de la Información se desarrolla, se implementa y publica dentro de los lineamientos de la política de Gobierno Digital, legislaciones nacionales, internacionales, procesos y procedimientos definidos por el Departamento del Cesar.

i) La entidad, gestionará y otorgará los recursos necesarios para garantizar los tres (3) pilares fundamentales de la Seguridad de información, como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la entidad.

j) La alta gerencia estará atenta y monitoreará la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de todos los Funcionarios, Contratistas y Terceros.

k) La Entidad, en virtud de las directrices y políticas establecidas por la política de gobierno digital, cumplirá con los requisitos legales, reglamentarios y contractuales que haya a lugar, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

Artículo 5. Revisión: El Departamento del Cesar establece que la Política de Seguridad y Privacidad de la Información se debe revisar y actualizar, en el momento que la necesidad lo amerite o por sugerencia del comité Institucional de Gestión y Desempeño de la entidad.

Artículo 6. Roles y Responsabilidades: Los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política serán los cargos que se definen a continuación:

a) Todos los Funcionarios, Contratistas y Terceros que ejercen funciones con la entidad y previamente han sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información, son responsables del cumplimiento de las políticas, procedimientos y normatividad vigente definida por la entidad.

b) Es responsabilidad de todos los Funcionarios, Contratistas y Terceros, que hagan uso de los equipos de cómputo del Departamento del Cesar, almacenar toda la información en la carpeta Mis Documentos que se encuentra ubicada en su equipo de cómputo, como resultado de sus funciones laborales.

c) Todos los Funcionarios, Contratistas y Terceros de la entidad, deben hacer buen uso de la información que se genera del desempeño de sus funciones laborales y bajo ninguna circunstancia podrán divulgar información clasificada o reservada con categoría CONFIDENCIAL en espacios públicos o privados, mediante conversaciones o situaciones que puedan poner en riesgo la seguridad o el buen nombre del Departamento del Cesar. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en el Acuerdo de Confidencialidad, cláusula que estará reglamentada en el contrato de prestación de servicios con la Entidad.

d) Todos los activos de información del Departamento del Cesar deben tener su propietario, su custodio, y usuarios que deben estar debidamente identificados, esto de acuerdo a que sólo los Líderes de Proceso definidos en el mapa de procesos de la Entidad, son los que pueden desempeñar las veces de propietarios de activos de información, de acuerdo a esto son los responsables de tomar las medidas necesarias para la protección de la disponibilidad, confidencialidad e integridad de la información de los activos.

e) El Grupo de Recursos Físicos y Tecnológicos definirá la Matriz de Roles y Responsabilidades para cada procedimiento de sistemas de información de

infraestructura tecnológica, en la cual se deben incluir los roles y sus privilegios, con el fin de crear el procedimiento de solicitud, modificación y eliminación de cuentas de usuario.

f) Si después de revisar la solicitud, se identifica que los privilegios solicitados no están definidos en la Matriz de Roles y Responsabilidades, se debe solicitar aprobación de privilegios por parte del líder del Proceso.

g) Todas las solicitudes deben tener fecha de finalización y cuando sean roles que no se encuentren en la Matriz serán considerados como Privilegios Temporales.

h) La solicitud de usuario y contraseña para la asignación de roles y privilegios la debe solicitar el líder de cada área, al Grupo de Recursos Físicos y Tecnológicos a través del correo electrónico institucional informatica@cesar.gov.co o Control Doc.

i) Los contratistas de la entidad tendrán usuario y contraseña para acceder a los sistemas de información solo si para el desarrollo de las actividades definidas en su contrato así lo requieran, previa solicitud hecha por el líder del área.

j) El Grupo de Recursos Físicos y Tecnológicos de la entidad, dará respuesta a las solicitudes de usuarios y contraseña en un periodo menor o igual a tres días hábiles.

k) La Matriz de Roles y Responsabilidades debe ser actualizada en el momento que así se requiera, de acuerdo a un requerimiento formal por parte del Líder del Proceso o Responsable del Activos de Información.

l) Todos los requerimientos deben ser solicitados formalmente a través del procedimiento establecido de creación de cuentas de usuarios.

Artículo 7. Reporte de incidente ante las autoridades. El Departamento del Cesar a través de este procedimiento debe especificar cuándo, cómo y ante qué autoridades se deben hacer los reportes de incidentes identificados en materia de seguridad de información.

CAPITULO III
Política de Dispositivos Móviles

Artículo 8. Objetivo: Proteger la información almacenada en dispositivos móviles de propiedad del Departamento del Cesar.

La política de dispositivos móviles está formada por los siguientes controles que se relacionan a continuación:

a) Se debe llevar un registro y control de todos los dispositivos móviles que posee la Entidad.

b) Todos los Funcionarios, Contratistas y Terceros, deben hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones.

c) El uso de dispositivos móviles fuera de las instalaciones de la entidad sólo será autorizado por el líder de cada área.

d) Los dispositivos móviles que estén autorizados para salir y que contengan información sensible, se deben proteger mediante el uso de controles tecnológicos apropiados para ello, como contraseña o clave, políticas de Restricción en la ejecución de aplicaciones, y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

e) En todos los dispositivos móviles de propiedad de la entidad, queda prohibido la instalación de software no autorizado, la instalación de juegos o cualquier otro tipo de software que no tenga relación con las funciones del cargo del profesional que tiene asignado el equipo.

f) El responsable de autorizar la instalación de software en los dispositivos móviles de propiedad de la entidad, es el grupo de Recursos Físicos y Tecnológicos de la entidad.

g) El profesional que tenga a su cargo un dispositivo móvil de propiedad de la entidad, debe velar por la seguridad física de este, evitar colocarlos en zona húmedas o de altas temperaturas, no debe transitar en zona de alto riesgo, minimizar la pérdida o robo del mismo.

h) Todos los dispositivos móviles de propiedad de la entidad que contengan información, deben tener instalado un software de antivirus.

i) En caso de pérdida o robo de un dispositivo móvil que contenga información de la entidad, el Funcionario, Contratistas o Tercero que tiene a cargo el dispositivo móvil, debe avisar inmediatamente al líder del área, para que se realicen las denuncias pertinentes al caso.

j) El Funcionario, Contratistas o Tercero, responsable del dispositivo móvil, debe hacer periódicamente copias de seguridad y guardarla como respaldo en un lugar seguro en su entorno de trabajo.

k) Todos los Funcionarios, Contratistas y Terceros, son responsables de garantizar el buen uso y servicio de los dispositivos móviles en redes seguras, y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

l) Todos los dispositivos móviles propiedad de los Funcionarios, Contratistas y Terceros, que requieran tener acceso a la red wifi de la entidad, deben solicitar autorización, mediante el procedimiento formal de autorización de ingreso a la red y estar debidamente identificados, con el fin de llevar el control y garantizar que se implementen las medidas de aseguramiento necesarias definidas por el Grupo de Recursos Físicos y Tecnológicos.

CAPITULO IV
Política de Gestión de Activos de Información

Artículo 9. Objetivo: Crear cultura a los funcionarios, Contratistas y Terceros sobre las acciones a realizar en cuanto al uso, administración y responsabilidad en materia de Gestión de Activos de Información.

Artículo 10. Identificación de Activos de Información: El Departamento del Cesar, realizará la actualización del inventario de Activo de información, en el momento que la necesidad lo requiera, bajo la responsabilidad del líder del área Archivo y el Grupo de Recursos Físicos y Tecnológicos, utilizando un instrumento que permita la clasificación de activo de información.

Artículo 11. Devolución de los Activos: Todos los Funcionarios, Contratistas y Terceros que ingresen a trabajar con el Departamento del Cesar, en el contrato de prestación de servicios o Acta de posesión, debe incluirse una cláusula, donde se comprometan entregar los activos físicos y la información, al líder del área, una vez finalizando la relación laboral con la entidad.

Artículo 12. Disposición de los Activos: La entidad a través de la política de seguridad, establecerá el procedimiento que le permita a los funcionarios, Contratistas y Terceros,

contar con unos lineamientos claros que garanticen la toma de decisiones, con el fin de realizar acciones que conduzcan a mitigar el riesgo en materia de activos de información, esta política incluirá dentro del procedimiento la correcta eliminación, retiro o traslado, cuando ya no se necesiten los activos.

CAPITULO V
Política de Seguridad de los Recursos Humanos

Artículo 13. Objetivos: Garantizar la protección, disponibilidad, integridad y confidencialidad de la información del personal que trabaja para el Departamento del Cesar, a través de mecanismos de validación y concientización del recurso humano que hará uso de la misma.

Artículo 14. Control y Política del Personal: Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de la entidad, de igual forma darle a conocer su responsabilidad en materia de Seguridad y Privacidad de la información.

Artículo 15. Acuerdo de Confidencialidad: Todos los Funcionarios, Contratistas y Terceros que ingresen a trabajar con el Departamento del Cesar, en el contrato de prestación de servicios o Acta de posesión debe incluirle una cláusula de Confidencialidad o no divulgación de información. Este acuerdo debe contener la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, en el tratamiento de la información por parte de la entidad. De igual forma el Departamento del Cesar dentro del mismo acuerdo establecerá los siguientes controles que se relacionan a continuación:

a) Todas las personas que ingresen a trabajar con el Departamento del Cesar, en el contrato de prestación de servicios o Acta de posesión declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del Funcionario, Contratistas o Tercero.

b) La entidad, a través de sus canales de comunicación informará a los funcionarios, contratistas y terceros, la importancia de cumplir la política de Seguridad y Privacidad de la Información con el fin de que tomen conciencia y la pongan en práctica.

Artículo 16. Proceso disciplinario: Cuando exista una violación de las políticas de seguridad y privacidad de la información, la entidad se reserva el derecho de aplicar las medidas disciplinarias, acordes a los compromisos laborales de los funcionarios, Contratistas y Terceros, dentro del marco legal a que haya lugar.

CAPITULO VI
Política de uso de correo electrónico

Artículo 17. Objetivo: Definir las directrices generales del buen uso del correo electrónico en el Departamento del Cesar.

Artículo 18. Usos aceptables del servicio: Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar al interior de la entidad y no se debe utilizar para otros fines. Dentro del mismo uso aceptable del servicio se establecen los siguientes controles que se relacionan a continuación:

a) Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen del Departamento del Cesar.

b) Todos los Funcionarios, Contratistas y Terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten en sus buzones de correo electrónico.

c) Todos los Funcionarios, Contratistas y Terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la entidad.

d) El servicio de correo electrónico institucional debe ser empleado para servir a una finalidad operativa y administrativa en relación con la entidad. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad, que se consideran de propiedad del Departamento del Cesar pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

e) Cuando un Proceso, Oficina, Grupo o Dependencia, tenga información de interés institucional en materia de seguridad de información para divulgar, lo debe hacer a través de El Grupo de Recursos Físicos y Tecnológicos de la entidad, utilizando el medio formal autorizado para realizar esta actividad.

f) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la entidad y deberán conservar en todos los casos el mensaje legal corporativo.

g) El único servicio de correo electrónico controlado en la entidad es el asignado directamente por el Grupo de Recursos Físicos y Tecnológicos , el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

h) Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de Todos los Funcionarios, Contratistas y Terceros.

i) El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por El Grupo de Recursos Físicos y Tecnológicos de la entidad.

j) Es responsabilidad de las personas que utilizan los correos electrónicos institucionales, estar monitoreando su bandeja de entrada con el fin de evitar el llenado de la misma.

k) Todos los Funcionarios, Contratistas y Terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de la entidad, para que de esta forma el Grupo de Recursos Físicos y Tecnológicos realice el ajuste de permisos requerido.

l) El usuario debe reportar al Grupo de Recursos Físicos y Tecnológicos de la entidad, cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos, de igual forma los usuarios deben reportar cualquier comportamiento inusual que observen en su correo electrónico.

m) Cuando un funcionario o contratista se retire de la entidad y se le haya autorizado el uso de una cuenta de correo electrónico Institucional, debe abstenerse de continuar empleándola y se debe verificar que su cuenta de acceso a los servicios sean cancelados.

n) Los mensajes y la información contenida en los buzones de correo electrónicos institucionales son de propiedad del Departamento del Cesar.

ñ) Cada usuario debe asegurar que en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios correspondientes.

o) Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

p) Todo usuario es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Funcionario, Contratistas o Tercero desconfíe del remitente de un correo electrónico, debe remitir la consulta al Grupo de Recursos Físicos y Tecnológicos.

q) Si una cuenta de correo electrónico es interceptada por personas mal intencionadas, o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), El Grupo de Recursos Físicos y Tecnológicos actuará según sea el caso.

r) El Grupo de Recursos Físicos y Tecnológicos se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico Institucional para evitar amenazas de virus y otros programas destructivos.

s) Ningún Funcionario, Contratistas o Tercero debe suscribirse en boletines en líneas, publicidad o que no tengan que ver con sus actividades laborales, con el correo institucional.

t) El Funcionario, Contratistas o Tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario debe notificar al Grupo de Recursos Físicos y Tecnológicos, con el fin de que ejecuten las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo electrónico de la entidad.

Artículo 19. Usos no aceptables del servicio: Envío de correos masivos que no hayan sido previamente autorizados por el Grupo de Recursos Físicos y Tecnológicos de la entidad. De igual forma dentro del uso no aceptable del servicio se establecen los siguientes controles que se relacionan a continuación:

a) Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.

b) Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de la seguridad de información.

c) Envío o intercambio de mensajes que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

d) Envió de mensajes que contengan amenazas o mensajes violentos.

e) Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

f) Divulgación no autorizada de información propiedad del Departamento del Cesar.

g) Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

h) Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

i) Adulterar o intentar adulterar mensajes de correo electrónico.

j) Enviar correos masivos, con excepción de funcionarios con nivel de Director o superior, quienes sean previamente autorizados por estos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.

CAPITULO VII
Política de uso de Internet

Artículo 20. Objetivo: Definir los lineamientos generales para el buen uso del internet y asegurar una adecuada protección de la información del Departamento del Cesar.

Artículo 21. Usos aceptables del servicio: La solicitud del servicio de internet, se debe hacer mediante el procedimiento formal establecido para tal fin, de igual forma para el uso aceptable del servicio, se establecen los siguientes controles que se relacionan a continuación:

a) Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación con la entidad y no debe utilizarse para ningún otro fin.

b) Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos o que afecte la seguridad de la información de la entidad.

c) Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

d) El navegador autorizado para el uso de Internet en la red de la entidad es el instalado por el Grupo de Recursos Físicos y Tecnológicos, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.

e) No se permite la conexión de módems externos o internos en la red del Departamento del Cesar, salvo previa solicitud autorizada por el Grupo de Recursos Físicos y Tecnológicos de la entidad.

f) Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades al interior de la entidad.

g) Para realizar intercambio de información de propiedad del Departamento del Cesar con otras entidades, se debe seguir un proceso formal de solicitud de información, el cual debe contar con la previa autorización del líder del área.

h) La entidad, se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

i) Todos los usuarios que se encuentren autorizados son responsables de hacer un uso adecuado de este recurso y por ninguna razón se pueden realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, y las políticas de seguridad de la información, entre otros.

j) Los Funcionarios, Contratistas y Terceros del Departamento del Cesar no deben asumir en nombre de la entidad, posiciones personales en encuestas de opinión, foros u otros medios similares.

k) Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la entidad.

Artículo 22. Usos no aceptables del servicio: El Departamento del Cesar no permitirá el mal uso del servicio del internet, conductas y acciones que contradigan la política de seguridad y privacidad de la información, por lo tanto dentro del uso no aceptable del servicio, se establecen los siguientes controles que se relacionan a continuación:

a) Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

b) Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

c) Cualquier otro propósito diferente al considerado en el apartado de usos aceptables del servicio de la presente política.

d) Todos los usuarios invitados que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

e) No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, hardware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos del Departamento del Cesar y las emitidas por los entes de control.

f) No se permite la descarga de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

CAPITULO VIII
Política de uso de Redes Sociales

Artículo 23. Objetivos: Definir los lineamientos generales para el uso de los servicios de Redes Sociales por parte de los usuarios autorizados al interior de la entidad.

Artículo 24. Usos aceptables del servicio: Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del Departamento del Cesar. El Departamento del Cesar para el uso aceptable de las redes sociales, establece los siguientes controles que se relacionan a continuación:

a) El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con el Departamento del Cesar. Todas las comunicaciones

establecidas mediante este servicio deben ser monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control que lo requiera.

b) El acceso a redes sociales queda sujeto a la solicitud hecha por el líder del área siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.

c) El Grupo de Recursos Físicos y Tecnológicos de la entidad, será el encargado de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en el Departamento del Cesar.

Artículo 25. Usos no aceptables del servicio: El Departamento del Cesar no acepta el uso de las redes sociales, cuando estas no son utilizadas para el desarrollo de actividades relacionado con el cargo, por lo anterior establece los siguientes controles que se relacionan a continuación:

a) No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

b) No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.

c) No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet del Departamento del Cesar, o aprovechar el acceso a Redes Sociales para fines ilegales.

d) No se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

CAPITULO IX
Política de uso de Recursos Tecnológicos

Artículo 26. Objetivo: Definir los lineamientos generales para el uso aceptable de los recursos tecnológicos del Departamento del Cesar

Artículo 27. Usos aceptables del servicio: La entidad, asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los Funcionarios, Contratistas y Terceros de ser necesario, de igual forma establece los controles para el uso aceptable de los recursos tecnológicos que se relacionan a continuación:

a) La instalación de software se encuentra bajo la responsabilidad del Grupo de Recursos Físicos y Tecnológicos de la entidad, y por tanto son los únicos autorizados para realizar esta actividad.

b) El Grupo de Recursos Físicos y Tecnológicos de la entidad, es el responsable de la instalación, desinstalación y actualización de cualquier tipo de software y aplicaciones que se encuentren o se quieran instalar en los equipos de cómputos de la entidad. Así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

c) Sólo el personal autorizado por el Grupo de Recursos Físicos y Tecnológicos, podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la entidad; las conexiones establecidas para este fin, utilizan los esquemas de seguridad establecidos por la entidad.

d) Los Funcionarios, Contratistas y Terceros de la Entidad son responsables de hacer buen uso de los recursos tecnológicos del Departamento del Cesar, y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros Funcionarios, Contratistas y Terceros, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por la entidad.

e) Todo activo de propiedad de la entidad, asignado a Funcionarios, Contratistas y Terceros, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.

Artículo 28. Usos no aceptables del servicio: El Departamento del Cesar para el uso no aceptable de los recursos tecnológicos establece el siguiente control que se relaciona a continuación:

1. Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, estos cambios únicamente deben ser realizados por el Grupo de Recursos Físicos y Tecnológicos de la entidad.

CAPITULO X
Política de Clasificación de Información

Artículo 29. Objetivo: Asegurar que la información clasificada del Departamento del Cesar, sea tratada y protegida adecuadamente.

Artículo 30. Esquema de Clasificación de la Información: Toda la información del Departamento del Cesar debe ser identificada y clasificada de acuerdo a los niveles de clasificación de información establecida o adoptado por la entidad, de igual forma se establecen los siguientes controles en materia de clasificación y almacenamiento de información:

a) Acceso a la información sólo de personal autorizado.
b) Llevar un registro formal de acceso a la información.
c) Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

Artículo 31. Etiquetado y manejo de Información: Los líderes de cada área deben delegar a quien corresponda, mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental, para tal fin se establecen los controles que se relacionan a continuación:

a) Los líderes de cada área delegarán a quien corresponda, realizar las acciones que conduzcan garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

b) Todos los Funcionarios, Contratistas y Terceros de la entidad son responsables de la organización, conservación, uso y manejo de los documentos.

c) Todas las dependencias del Departamento del Cesar deben enviar al Archivo Central, la documentación de forma ordenada y organizada, de acuerdo a los tiempos establecidos en la Tabla de Retención Documental y el Manual de Gestión Documental, acompañado del formato único de inventario documental FUID.

d) El Archivo Central del Departamento del Cesar recibe las transferencias documentales de acuerdo al cronograma anual de transferencia Documentales.

e) Los archivos de Gestión de las oficinas del Departamento del Cesar deben custodiar sus documentos de acuerdo a lo especificado en las tablas de Retención Documental.

f) La plataforma tecnológica usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos, debe garantizar los principios fundamentales de la seguridad como son: la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.

g) El etiquetado de información debe incluir la información física y electrónica.

h) Las etiquetas de la información, se deben identificar y reconocer fácilmente.

i) Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

Artículo 32. Usos no aceptables: El Departamento del Cesar no acepta acciones o actitudes, que pongan entre dicho la clasificación de activo de información de la entidad, por tal razón relaciona a continuación los usos no aceptables:

a) Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos, solicitudes y denuncias. De igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.

b) Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.

c) Divulgación no autorizada de los expedientes, documentos, información o archivos.

d) Realizar actividades tales como borrar, modificar, alterar o eliminar información del Departamento del Cesar de manera mal intencionada.

CAPITULO XI
Política de gestión de medios de almacenamiento

Artículo 33. Objetivo: Proteger la información del Departamento del Cesar, velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Artículo 34. Gestión y Disposición de medios removibles: Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de la entidad y uso hasta finalización de su contrato o cese de actividades, de igual forma el Departamento del Cesar establece los siguientes controles en materia de gestión de medios de almacenamiento que se relacionan a continuación:

a) Toda la información clasificada como publica reservada y publica clasificada que sea almacenada en medios removibles y que se requiera de protección especial, debe cumplir con las directrices de seguridad emitidas por el Grupo de Recursos Físicos y Tecnológicos específicamente aquellas referentes al empleo de técnicas de cifrado.

b) Se debe llevar un registro actualizado de todos los medios removibles de la entidad, incluyendo el nombre del funcionario o contratista que lo tiene a su cargo.

c) Todos los medios removibles deben ser almacenados de manera segura.

d) Los medios de almacenamiento removibles que se conecten a la red de datos del Departamento del Cesar o que se encuentren bajo su custodia, están sujetos a monitoreo por parte del Grupo de Recursos Físicos y Tecnológicos de la entidad.

e) Todos los dispositivos de almacenamiento removibles (Discos Duros, Memorias USB) que pertenezcan al Departamento del Cesar, y que requieran salir de la entidad, el funcionario que lo tenga a su cargo, deberá informar a su jefe inmediato con copia a la oficina de almacén.

f) Todos los medios de almacenamiento removibles propiedad de la entidad, deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

g) Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc., con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

h) Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por la entidad, para su uso dentro de la red corporativa, podrán ser revisados Grupo de Recursos Físicos y Tecnológicos.

i) Todos los medios de almacenamiento que contengan información del Departamento del Cesar y equipos que vayan a ser dados de baja, el Grupo de Recursos Físicos y Tecnológicos debe garantizar que la información contenida en dicho dispositivo fue eliminada sin poder ser restaurada. (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores, discos duros externos, etc.).

j) Los medios de almacenamiento que contengan información de la entidad y que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por el Departamento del Cesar, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).

Artículo 35. Transferencia de medios físicos: El Departamento del Cesar para la transferencia de medios físicos establece los siguientes controles que se relacionan a continuación, que permiten garantizar la confidencialidad, integridad y disponibilidad de la información de la entidad.

a) Toda la información clasificada como publica reservada y publica clasificada que se desee almacenar en medios removibles y que sean transportados fuera de las instalaciones del Departamento del Cesar, debe cumplir con las disposiciones de seguridad indicadas por el Grupo de Recursos Físicos y Tecnológicos de la entidad, específicamente aquellas referentes al empleo de técnicas de cifrado.

b) El transporte de los medios físicos, se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma evitar una afectación a la integridad y disponibilidad de la información.

c) Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.

CAPITULO XII
Política de Control de Acceso

Artículo 36. Objetivo: Definir las directrices generales para un acceso controlado a la información del Departamento del Cesar.

Artículo 37. Control de Acceso a Redes y Servicios en Red: La entidad suministra a los usuarios, las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales, en ese mismo sentido el Departamento del Cesar estable los siguientes controles que se relacionan a continuación en materia de control de acceso de información:

a) Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

b) Sólo el personal designado por el Grupo de Recursos Físicos y Tecnológicos de la entidad, está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de tecnológica

c) Toda actividad que requiera acceder a los servidores, equipos o a las redes de la entidad, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización por el Grupo de Recursos Físicos y Tecnológicos.

d) La conexión remota a la red de área local, debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por el Grupo de Recursos Físicos y Tecnológicos, que cuenta con el monitoreo y registro de las actividades necesarias.

e) La creación y retiro de usuarios en los sistemas de información, debe seguir un procedimiento de creación, edición y eliminación de usuarios.

f) Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

Artículo 38. Gestión de Acceso a Usuarios: Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración y se determinan los siguientes controles que se relacionan a continuación:

a) Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

b) Las contraseñas deben contener mayúsculas, minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.

c) Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la mesa de servicios.

d) Todos los usuarios deben dar buen uso a las claves de acceso y son los responsable por el uso de su contraseña.

e) Se deben cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo impresoras, routers, switch, herramientas de seguridad, etc.).

f) No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.

g) Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información, de uso y selección de las contraseñas de acceso, por lo tanto son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

h) Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

i) Reportar al Grupo de Recursos Físicos y Tecnológicos de la entidad, sobre cualquier incidente o sospecha que otra persona esté utilizando su contraseña o usuario asignado.

j) Reportar al Grupo de Recursos Físicos y Tecnológicos de la entidad, sobre cualquier sospecha o evidencia que una persona esté utilizando una contraseña y usuario que no le pertenece.

k) Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada tres (3) meses.

l) El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por el Grupo de Recursos Físicos y Tecnológicos de la entidad.

Artículo 39. Revisión de los derechos de acceso de los Usuarios: Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de Procesamiento de Información de la entidad, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

Artículo 40. Retiro de los derechos de acceso: La Oficina de Talento Humano y Gestión Contractual son las encargadas de comunicar al grupo de Recursos Físicos y Tecnológicos de la entidad sobre las novedades de los funcionarios, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

CAPITULO XIII
Política de Seguridad Física y del Entorno

Artículo 41. Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información del Departamento del Cesar.

Artículo 42. Perímetro de Seguridad Física: Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los Funcionarios, Contratistas y Terceros autorizados, evitar que las puertas se dejen abiertas, de igual forma la entidad establece los siguientes controles en materia de seguridad física y del entorno, que se relacionan a continuación:

a) Todos los Funcionarios, Contratistas y Terceros cuando sea el caso, sin excepción deben portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de la entidad.
b) Es responsabilidad de todos los Funcionarios, Contratistas y Terceros del Departamento del Cesar borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas que comprometan la seguridad de la información sobre las mesas al finalizar las reuniones.

c) Los visitantes que requieran permanecer en las oficinas de la entidad por periodos superiores a dos (2) días, deben ser presentados al personal de oficina donde permanecerán.

d) Los dispositivos removibles, así como toda información CONFIDENCIAL del Departamento del Cesar, independientemente del medio en que se encuentre, deben permanecer guardados bajo seguridad durante horario no hábil o en horarios en los cuales el Funcionarios, Contratistas o Terceros responsable no se encuentre en su sitio de trabajo.

Artículo 43. Controles de Acceso Físico: Las áreas seguras, dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

Artículo 44. Servicio de Vigilancia Privada: El personal de vigilancia privada contratado por el Departamento del Cesar, debe garantizar las acciones de control de acceso, revisión y registro documentado de los componentes de TI que ingresen y salgan de la entidad.

Artículo 45. Uso no aceptable: En las áreas seguras, bajo ninguna circunstancia se puede fumar, comer o beber.

Artículo 46. Ubicación y Protección de los equipos: La plataforma tecnológica (hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Artículo 47. Protección eléctrica: La entidad debe contar con sistemas de control protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Artículo 48. Seguridad de los equipos fuera de las instalaciones: Los equipos portátiles que pertenezcan a la entidad y que contengan información clasificada como publica reservada y publica clasificada, deben estar protegidos con claves de usuarios y contraseña, en ese mismo sentido la entidad establece los siguientes controles que se relacionan a continuación:

a) Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

b) En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al Proceso de Gestión Administrativa y al Grupo de Recursos Físicos y Tecnológicos de la entidad, y el afectado debe poner la denuncia ante las autoridades competentes y hacer llegar copia de la misma a su jefe inmediato.

c) Cuando los equipos portátiles se encuentren desatendidos dentro o fuera de las instalaciones de la entidad, estos deben estar asegurados a través de guayas.

d) Todos los equipos de cómputo de la entidad, deben ser registrados al ingreso y al retirarse de las instalaciones del Departamento del Cesar.

Artículo 49. Reasignación de equipo de cómputo: Se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

Artículo 50. Equipo de cómputo dado de baja: Se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, el Grupo de Recursos Físicos y Tecnológicos informará a la oficina de almacén las causales que

motivaron darle de baja al equipo de cómputo, con el fin de realizar el respectivo descargue al funcionario respectivo.

Artículo 51. Retiro de Activos: Ningún equipo de cómputo, debe ser retirado de la entidad sin una autorización formal.

CAPITULO XIV
Política de Escritorio y Pantalla Despejada

Artículo 52. Objetivo: Definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información del Departamento del Cesar, de igual forma la entidad establece los siguientes controles de escritorio despejado y pantalla despejada que se relacionan a continuación:

a) Todo el personal de la entidad debe conservar su escritorio libre de información, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento, el contenido del fondo del escritorio del PC debe tener contener imagen de fondo relacionada con la entidad.

b) Todo el personal de la entidad debe bloquear la pantalla de su equipo de cómputo, cuando no estén haciendo uso de ellos, o que por cualquier motivo deban dejar su puesto de trabajo.

c) Todos los usuarios al finalizar sus actividades diarias, deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

d) Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

e) En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

CAPITULO XV
Política de Gestión de Cambios

Artículo 53. Objetivo: Asegurar que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en el Departamento del Cesar se realicen de forma controlada, de igual forma la entidad para la política de gestión de cambios, la entidad establece los siguientes controles que se relacionan a continuación:

a) Se deben establecer procedimientos para el control de cambios ejecutados en la entidad.

b) Toda solicitud de cambio en los servicios de procesamiento de información de la entidad, se debe realizar siguiendo el procedimiento de gestión de cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.

c) Se debe llevar una trazabilidad del control de cambios solicitados.

d) En el procedimiento de gestión de cambios se debe especificar los canales autorizados para la recepción de solicitudes de cambios, como la mesa de servicios, correo electrónico o un oficio dirigido al responsable del Grupo de Recursos Físicos y Tecnológicos de la entidad.

e) Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.

f) Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.

g) Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los Funcionarios, Contratistas o Terceros que por sus funciones tienen relación con el sistema de información.

h) Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

i) Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

j) Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abordar los cambios y volver al estado anterior.

CAPITULO XVI
Política de prueba de software y sistemas de información antes de su implementación

Artículo 54. Objetivo: Reducir riesgos asociados en cuanto a funcionamiento, aplicabilidad y seguridad en los sistemas de adquisición de la entidad. El Departamento del Cesar establece los siguientes controles en materia de prueba de software y sistemas de información que se relacionan a continuación:

a) El Departamento del Cesar debe establecer y mantener ambientes separados de verificación y pruebas de software, dentro de la infraestructura de soporte técnico. Esto aplica para los Software que contengan información catalogada con criticidad alta de acuerdo al inventario y clasificación de activos de información.

b) El ambiente de verificación y prueba de software se debe utilizar para propósitos de implementación, parametrización, cambio, modificación y ajuste. Por su parte, el ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de Software. Por último el ambiente de verificación y pruebas de software, debe utilizarse para la prestación del servicio que involucre el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la entidad.

c) Los Software a la medida antes del recibido a satisfacción, deben ser validados de tal forma que nos permita garantizar el objetivo para la cual fue adquirido.

d) Los Software y Sistemas de información en la fase de entrega a satisfacción, deben contar con los respectivos manuales de usuarios.

e) Todo software, hardware, cableado estructurado, bienes o servicios a fines que el Departamento del Cesar piense adquirir debe ser revisado previamente por el del Grupo de Recursos Físicos y Tecnológicos.

CAPITULO XVII
Política de protección contra código malicioso

Artículo 55. Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos al interior de la entidad. El Departamento del Cesar en materia de protección contra código malicioso establece los siguientes controles que se relacionan a continuación:

a) Toda la infraestructura de procesamiento de información de la entidad, debe contar con un sistema de detección y prevención de intrusos, herramienta de anti-spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

b) Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de la entidad.

c) Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.

d) Todos los Funcionarios, Contratistas y Terceros que hacen uso de los servicios de Tecnología de la Información y Comunicaciones de la entidad, son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

e) El Departamento del Cesar debe contar con firewall y software necesario, como son los antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por Grupo de Recursos Físicos y Tecnológicos

f) Los antivirus adquirido por la entidad, sólo debe ser instalados por los responsables del Grupo de Recursos Físicos y Tecnológicos

g) Los equipos de terceros que son autorizados para conectarse a la red de datos de la entidad, deben tener antivirus y contar con las medidas de seguridad apropiadas.

h) La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

i) Se deben hacer campañas de sensibilización a todos los Funcionarios, Contratistas y Terceros del Departamento del Cesar, con el fin de generar una cultura de seguridad de la información.

j) Los Funcionarios, Contratistas y Terceros del Departamento del Cesar, pueden realizar acciones frente a circunstancia sospechosas de contener software malicioso. En cualquier caso, los Funcionarios, Contratistas y Terceros cuando sea necesario siempre podrán consultar al Grupo de Recursos Físicos y Tecnológicos de la entidad, sobre el tratamiento que debe darse en caso de sospecha de malware.

k) Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

l) Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por el Departamento del Cesar, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución; en estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, y se debe informar al Grupo de Recursos Físicos y Tecnológicos de la entidad.

m) El único servicio de antivirus autorizado en la entidad es el asignado directamente por el Grupo de Recursos Físicos y Tecnológicos de la entidad, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para minimizar ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por el Grupo de Recursos Físicos y Tecnológicos, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

n) El Grupo de Recursos Físicos y Tecnológicos es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red de la entidad.

ñ) El Grupo de Recursos Físicos y Tecnológicos se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o transporten y almacenen en cualquier medio, en busca de virus o código malicioso.

o) El Grupo de Recursos Físicos y Tecnológicos se reserva el derecho de filtrar los contenidos que se trasmitan en la red de la entidad, con el fin de evitar amenazas de virus.

p) Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

CAPITULO XVIII
Política de Backup

Artículo 56. Objetivo: Proporcionar medios de respaldo de información adecuados por el Departamento del Cesar para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla, en ese sentido la entidad establece los controles que se relacionan a continuación:

a) El Grupo de Recursos Físicos y Tecnológicos, debe realizar periódicamente un análisis de las necesidades del negocio para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.

b) El Grupo de Recursos Físicos y Tecnológicos de la entidad, y el responsable de Seguridad de la Información junto a los propietarios de la información deben determinar los requerimientos para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de TI.

c) El Grupo de Recursos Físicos y Tecnológicos, debe disponer y controlar la ejecución de las copias de servidores, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de la entidad.

d) El dueño de la información es responsable de realizar periódicamente respaldo de la misma, en caso de no tener los conocimientos para hacerlo deberá solicitar el apoyo del Grupo de Recursos Físicos y Tecnológicos.

e) Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

f) Se deben definir procedimientos para el respaldo de la información, que incluyan los siguientes parámetros:

1. Establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

2. Almacenar en una ubicación remota (nube) o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.

3. Para realizar las copias de respaldo en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado por la Entidad a los que se encuentre sujeta.

4. Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.

5. Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.

g) El Grupo de Recursos Físicos y Tecnológicos de la entidad, a través del Administrador de Bases de Datos, de la Red y servidores, debe:

1. Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.

2. Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.

3. Realizar una copia de respaldo incremental diaria de los Servidores de Base de Datos, servidores Web, Sistemas de Información misionales, Aplicaciones, Desarrollo y dispositivos de red y consolidar una semanal.

4. Las copias de respaldo se deben realizar en horario no hábil, lo cual será verificado a través de Procesos Automáticos.

5. Los dispositivos magnéticos que contienen información crítica, deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.

6. El sitio alterno donde se almacenan las copias de respaldo, debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados.

7. Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.

8. El Grupo de Recursos Físicos y Tecnológicos de la entidad, debe contar con una Copia Backup, para cada servidor en un sitio externo.

9. El Grupo de Recursos Físicos y Tecnológicos de la entidad, cuenta con un responsable para gestionar la entrega o retiro de las copias de respaldo Backup del sitio externo.

Artículo 57. Registro de Respaldo de Información: Debe existir un procedimiento formal de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo.

El Departamento del Cesar establece los siguientes controles en materia de respaldo de información que se relacionan a continuación:

a) Llevar el registro de los Respaldos de Información realizada de forma Diaria.

b) Registro del retiro de las copia de respaldo - Backup del sitio externo.

c) Registro del ingreso de las copia de respaldo - Backup al sitio externo.

d) Inventario de las copias de Respaldo – Backup

e) Comprobación de Integridad de la Información

f) La información respaldada debe ser probada como mínimo dos (2) veces al año, asegurando que es confiable, integra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.

g) Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.

h) Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.

i) El Grupo de Recursos Físicos y Tecnológicos de la entidad, a través del Administrador de la Base de Datos, de Red y Servidores, debe aplicar los siguientes lineamientos:

   1. Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.

   2. Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.

   3. Mantener siempre una copia de la información de los Servidores, por lo menos con una antigüedad no superior a 24 horas.

j) Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.

k) Todos los usuarios deben almacenar la información resultado de sus actividades laborales en la carpeta "Documentos" a la cual se realiza back-up.

l) Todos los usuarios son responsables de realizar los respaldos de información personal almacenada en los equipos asignados.

m) Todos los Funcionarios, Contratistas y Terceros del Departamento del Cesar deben dar estricto cumplimiento a esta política y el que haga caso omiso puede ser sujeto de acciones disciplinarias o civiles, incluyendo la terminación del respectivo contrato.

CAPITULO XIX
Política de eventos de auditoria

Artículo 58. Objetivo: Asegurar que los registros de los eventos y las operaciones realizadas sobre los Sistemas de Información y Plataforma Tecnológica de la entidad permitan contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

Artículo 59. Registro de eventos: Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones de la entidad, deben ser registrados.

Artículo 60. Eventos de auditoria: Se debe hacer copia de respaldo de información de los eventos de auditoria, ya que en caso de un incidente de seguridad de la información deben estar disponibles.

Artículo 61. Registro del administrador y del Operador: Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información de la entidad deben estar debidamente registradas.

Artículo 62. Cuenta de usuario exclusiva: Los administradores de la infraestructura tecnológica y de procesamiento de información deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración y debe ser entregada a través de un proceso formal.

Artículo 63. Sincronización de relojes: Todos los relojes de la infraestructura de procesamiento de información del Departamento del Cesar, deben estar sincronizados con la hora legal Colombiana.

CAPITULO XX
Política de gestión de seguridad de las redes

Artículo 64. Objetivo: Establecer los controles necesarios para proteger la información del Departamento del Cesar transportada desde la red interna, para esos la entidad establece los siguientes controles que se relacionan a continuación:

a) El Grupo de Recursos Físicos y Tecnológicos de la entidad, es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

b) La entidad proporciona a los Funcionarios, Contratistas y Terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el Grupo de Recursos Físicos y Tecnológicos.

c) El trabajo a través de medios remotos a la red de datos del Departamento del Cesar, sólo se permitirá de acuerdo a la Política de Teletrabajo establecida por la Entidad.

Artículo 65. Separación de Redes: La entidad debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información. En materia de separación de redes la entidad establece los siguientes controles que se relacionan a continuación:

a) Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.

b) Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

c) Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

d) Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

CAPITULO XXI
Política de seguridad de la información para las relaciones con los proveedores

Artículo 66. Objetivos: Establecer los criterios de seguridad la información para la información accedida por los proveedores.

Artículo 67. Acuerdo de servicios: En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar Acuerdos de Confidencialidad sobre el manejo de la información, para eso la entidad establece los controles que se relacionan a continuación:

a) Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

b) Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

CAPITULO XXII
Política de gestión de incidentes de seguridad de la información

Artículo 68. Objetivos: Gestionar todos los incidentes de seguridad de la información reportados en la entidad, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Artículo 69. Reporte sobre los eventos y las debilidades de la seguridad de la información: Todos los Funcionarios, Contratistas y Terceros de la entidad y terceras partes tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten, para tal fin la entidad establece los siguientes controles que se relacionan a continuación:

a) Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

b) Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

c) Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.

d) Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.

e) Para el transporte de elementos, se debe llevar la cadena de custodia.

f) Se deben documentar todos los incidentes de seguridad reportados.

g) Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

CAPITULO XXIII
Política de gestión de la continuidad del negocio

Artículo 70. Objetivos: Garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información del Departamento del Cesar, para eso la entidad establece los siguientes controles que se relacionan a continuación:

a) La entidad debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.

b) El Grupo de Recursos Físicos y Tecnológicos gestionará ante la alta dirección la adquisición de servicios en la nube, para la instalación de sistemas de información y copias de seguridad.

Artículo 71. La presente resolución rige a partir de su publicación en la Gaceta Departamental y deroga la Resolución 0001534 del 10 mayo de 2010.

COMUNÍQUESE, PUBLIQUESE Y CÚMPLASE

Dado en Valledupar-Cesar a los 03 SEP 2019

FRANCISCO F. OVALLE ANGARITA
Gobernador Departamento del Cesar

Elaboró: Alex Enrique Gómez Garzón-Profesional Especializado
Revisó: Alfonso Garcia Payares-Profesional especializado
Aprobó: Luis José Rodríguez Torres, SED-Presidente Comité de Gestión y Desempeño del Departamento del Cesar.
Revisó: Ana Leidys Van-Strahlen Peinado- Jefe Oficina Asesora Jurídica
Revisó: Virginia Esther Ojeda Arboleda-Asesora Despacho