MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CORPOCESAR
CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR

SUBDIRECCIÓN GENERAL ÁREA DE PLANEACIÓN
OFICINA DE SISTEMAS Y TICS

TABLA DE CONTENIDO

1. OBJETIVO DEL MANUAL 3
2. ALCANCE DEL MANUAL 3
3. DEFINICIONES 3
4. POLÍTICAS 4
   - POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS 5
   - POLÍTICAS DE GESTIÓN DE ACTIVOS 5
   - POLÍTICAS DE CONTROL DE ACCESO LÓGICO 11
   - CRIPTOGRAFÍA 12
   - POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO 12
   - POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES 12
   - POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES 13
   - POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 13
   - POLÍTICAS DE RELACIONES CON LOS PROVEEDORES 14
   - POLÍTICAS DE GESTIÓN DE INCIDENTES 14
   - POLÍTICAS DE CUMPLIMIENTO 15
   - ESCRITORIO LIMPIO: 15
   - USO ADECUADO DE INTERNET 15
   - USO ADECUADO DE CORREO ELECTRÓNICO: 16
   - USO DE USUARIOS Y CONTRASEÑAS: 16
5. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN 17
   - SENSIBILIZACIÓN Y COMUNICACIÓN 17
   - CAPACITACIONES EN SEGURIDAD 17
6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS 17
7. SANCIONES 18

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR
CORPOCESAR

2023

1. OBJETIVO DEL MANUAL

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "**Política General de Seguridad de la Información de la Entidad**" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**.

2. ALCANCE DEL MANUAL

El presente manual de políticas aplica a funcionarios, contratistas, terceros, usuarios y visitantes de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** por alguna razón tengan cualquier tipo de interacción con los activos de información.

3. DEFINICIONES

- **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Seguridad Lógica:** Establece e integra los mecanismos y procedimientos, que permiten monitorear el acceso a los activos de información lógicos, que incluyen los controles de administración de usuarios, definición de

responsabilidades, perfiles de seguridad, control de acceso a los sistemas de información de acuerdo a las necesidades y funciones del usuario, análisis de incidentes de seguridad lógica y lecciones aprendidas de los mismos, monitoreo de aplicaciones críticas, análisis forense, documentación sobre sistemas, software malicioso, y además, participa en la definición de la arquitectura de las soluciones para garantizar el cumplimiento específico en los términos de seguridad de la información requeridos.

- **Seguridad Física:** Identifica los límites mínimos que se deben cumplir en cuanto a zonas seguras y perímetros de seguridad física, accesos físicos, control de ingreso y salida de activos, administración infraestructura locativa, entre otros, de forma que se puedan establecer controles que garanticen la seguridad de la información y del personal.
- **Activos de información:** Los activos de información en la compañía se clasifican de la siguiente manera: Software (incluye parametrizaciones, licencias, software genérico y a la medida, entre otros), hardware tecnológico, hardware no tecnológico (muebles, activos físicos, instalaciones, maestro de llaves, entre otros), información digital, documentación física, personas, intangibles (reputación, imagen, marca, good will, activos financieros, entre otros).
- **Continuidad de negocio:** La continuidad representa una serie de procesos coherentes encaminados a asegurar que la Entidad no experimente interrupciones inaceptables en cualquiera de sus operaciones esenciales, las cuales acarreen consecuencias financieras y operacionales e impacten negativamente a las partes interesadas.

4. POLÍTICAS

LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y

visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.
- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**.
- Los activos dispuestos por la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**. para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**.
- **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** identificara, clasificara y gestionara su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.

Identificación de Activos:

- El Líder de TI o quién haga sus veces en la entidad, será el responsable de la identificación y/o actualización del inventario de Activos de Información. Este proceso deberá ser realizado por lo menos una vez en cada vigencia, o en su defecto, a solicitud de algún líder de proceso de la entidad. El inventario de Activos de Información quedará registrado en el documento "**Inventario y Caracterización de Activos de Información**".

Clasificación de Activos:

- El Líder de TI o quién haga sus veces en la entidad, evaluará la clasificación de los Activos de Información de acuerdo a la criticidad, sensibilidad, reserva, integridad y disponibilidad de la misma, teniendo en cuenta la normativa vigente y aplicable a la Entidad, entre otras:
    - Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales"
    - Decreto 1377 de 2013: "Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015"
    - Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"
    - Decreto 103 de 2015 (*Derogado Parcialmente por el Decreto 1081 de 2015 - "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.*"): "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

Etiquetado de la Información:

- El Líder de TI o quién haga sus veces en la entidad junto con el Líder o dueño del proceso donde se encuentre el Activo de Información, deberán realizar el etiquetado de los Activos de Información de la siguiente forma: "Clasificado

Confidencialidad", "Clasificado Integridad" y "Clasificado Disponibilidad". En el caso de que un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.

Devolución de los Activos:

- El Líder de TI o quién haga sus veces en la entidad junto con los Líderes de Talento Humano, Oficina Jurídica y del Sistema Integrado de Gestión de la Calidad determinarán un instrumento que genere la obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad. El jefe Inmediato o quien haga sus veces sobre funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, convenio o contrato que se tenga con la entidad.

Gestión de medios removibles:

- El Líder de TI o quién haga sus veces en la entidad deberá establecer los mecanismos para restringir el uso de medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores de propiedad de CORPOCESAR. No deben usarse dispositivos de almacenamiento externos dañados y/o que presenten fallas y se deben mantener actualizados el antivirus y antimalware en los dispositivos a los que se conecte un medio removible.
- El uso de medios removibles en activos de la Corporación debe responder a la atención de una necesidad de la entidad y cuando no exista una alternativa adecuada. Entendiéndose que, para su uso se deben superar los riesgos asociados.

- La solicitud para el uso de un medio removible deberá comunicarse al jefe Inmediato para aprobación y luego al área de Sistemas y TICs, específicamente al Profesional Especializado encargado de la Seguridad Informática para realizar la evaluación previa a su aprobación final. Una mayor evaluación podría ser requerida para asegurar que es la solución adecuada. Ningún medio removible aprobado podrá ser conectado a un equipo externo a la entidad o fuera de la red. Toda excepción deberá ser aprobada por el área de Sistemas y TICs. El funcionario o servidor público es el responsable de la información contenida en los medios removibles que estén a su cargo como cintas, discos duros removibles, y dispositivos USB, que contengan información institucional, y la gestión deberá hacerse de acuerdo con las directrices impartidas en el proceso de Gestión Documental responsable de la disposición de los registros e información digital. Además, deben ser controlados y físicamente protegidos por el funcionario responsable de la información.
- Los usos de medios removibles en la entidad deben ir alineados a las clasificaciones de activos dispuestas en la presente política de Gestión de Activos.
- La información que es almacenada en medios removibles y que requiera estar disponible por largo tiempo, deberá estar protegida y controlada adecuadamente para evitar afectación por el tiempo de vida útil del medio.
- Los servidores públicos deberán devolver el medio removible a la Oficina de recursos Físicos o Almacén, previamente con el acompañamiento del área de Sistemas y TICs para asegurar un borrado seguro de la información contenida en el medio. Los dispositivos removibles que no sean requeridos o que estén dañados deben retornarse al área de Sistemas y TICs para realizar una evaluación técnica funcional para realizar un desecho seguro.
- Para evitar la fuga de información, los dispositivos removibles que funcionen deben limpiarse completamente con software y herramientas especializadas, eliminando toda la información antes de ser reutilizado. Los dispositivos que

presenten fallas deben deshabilitarse físicamente, previo a desecharse, para asegurar que la información no pueda rescatarse.

- Todo dispositivo de almacenamiento removible en uso (que contenga información de la Entidad) deberá ser encriptado. Excepciones por motivos misionales podrán darse previa comunicación y aprobación del área de Sistemas y TICs. El Líder de TI o quién haga sus veces en la entidad deberá proveer el software de encriptación, así como la guía para dicho proceso.
- Cualquier contraseña usada en un dispositivo removible debe cumplir con la Política de Contraseñas de la Corporación.
- Debido al alto riesgo de corrupción, mal funcionamiento o pérdida, los medios removibles no deben ser usados como almacenamiento primario. Se debe mantener en los sistemas de la Corporación una copia de toda la información almacenada en medios removibles.
- Todo dispositivo de almacenamiento removible en uso debe guardarse en un ambiente Seguro acorde al tipo y sensibilidad de la información contenida.
- Ante la sospecha de un dispositivo removible comprometido o si se confirma una infracción de seguridad (lo que incluye el mal funcionamiento, pérdida o robo) debe reportarse de inmediato a Soporte de TI con el fin de activar el Plan de Respuesta ante Incidentes de Seguridad.
- Ningún tercero (esto incluye, contratistas, proveedores, socios o agentes gubernamentales) puede acceder o extraer información de la Corporación con un medio removible sin el acuerdo explícito del área de Sistemas TICs y el dueño de la información. El uso de medios removibles por un tercero en cualquier activo de la Entidad debe pasar por una evaluación de riesgo y ser autorizado por el Profesional Especializado encargado de la Seguridad Informática.
- Si un tercero cuenta con la autorización para el uso de un medio removible, deberá cumplir con todas las consideraciones de esta política sobre el almacenamiento y transferencia de información. Los practicantes y recepcionistas tendrán los puertos USB deshabilitados.

Disposición de los activos:

- El Líder de TI o quién haga sus veces en la entidad deberá establecer un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos, deberá especificar el tipo de backup y su destinación. El jefe Inmediato del servidor público que haga la devolución decidirá la disposición de la información rescatada.

Dispositivos móviles:

- El Líder de TI o quién haga sus veces en la entidad evaluará la necesidad de utilización de dispositivos móviles (equipos portátiles, teléfonos móviles, tabletas, entre otros) para funcionarios de la entidad con el fin de facilitar el desempeño de sus labores. Asimismo, deberá implementar los controles de accesos, técnicas criptográficas para cifrar la información crítica almacenada en estos dispositivos móviles. Además, de mecanismos de respaldo de la información que contiene y demás consideraciones pertinentes para garantizar la seguridad de la información.
- Para realizar la instalación de chats y correos corporativos en teléfonos móviles o tabletas deberán registrar el dispositivo ante la oficina de Sistemas y TICs para que aplique los mecanismos de control de seguridad al dispositivo, entre los cuales se encuentra:
    - Instalar y configurar un antivirus.
    - Configurar el control de accesos al equipo con contraseña, lo que debe cumplir con la Política de Gestión de Accesos, en lo relacionado con el uso de contraseña, un patrón de seguridad de al menos 7 puntos de contacto o en su defecto la huella digital.
    - Configurar el bloqueo de la pantalla que no presente mensajes de alertas y que, al tener un tiempo de inactividad de dos minutos, se proceda a bloquear.

- En el caso de tener la propiedad de borrado de información remoto, se debe configurar con el fin de eliminar los datos del dispositivo, en caso de requerirlo, de forma remota.
- Realizar cifrado del dispositivo móvil.
- En el caso de pérdida o hurto de dispositivos móviles que se conecten a los servicios corporativos o almacenen información de CORPOCESAR deberán ser reportados a la oficina de Sistemas y TICs.
- Revisión del dispositivo para verificar el cumplimiento de la política.

- Las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles son, entre otras:
  - Hacer uso responsable del dispositivo móvil asignado.
  - Salvaguardar la integridad del dispositivo móvil.
  - Reportar comportamientos anormales o defectos que detecte en el dispositivo móvil.
  - No descargar ni instalar aplicaciones no autorizadas por la oficina de Sistemas y TICs.
  - No entregar el dispositivo móvil a externos para que realice operaciones sobre el equipo.
  - Cumplir con los lineamientos dados en esta política y las otras directrices impartidas por la entidad.

- Está prohibido almacenar información personal en los dispositivos móviles, al igual que está prohibido realizar la instalación de aplicaciones no autorizadas por la Oficina de Sistemas y TICs o la reinstalación del sistema operativo del equipo.

POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.

- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

CRIPTOGRAFÍA

- **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, el Grupo de Sistemas y Tecnologías de la Información y las Comunicaciones determinara los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** planea, gestiona, respalda y monitorea la

infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- El Grupo de Sistemas y Tecnologías de la Información y las Comunicaciones, establecerá los controles para acceso lógico y protección de las redes de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.
- La **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- El Grupo de Sistemas y Tecnologías de la Información y las Comunicaciones, velará que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.
- El Grupo de Sistemas y TICs generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

POLÍTICAS DE GESTIÓN DE INCIDENTES

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al Grupo de Sistemas y TICS por cualquiera de los medios dispuestos para tal fin.
- Sera responsabilidad del Grupo de Sistemas y Tecnologías de la Información y las Comunicaciones seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

POLÍTICAS DE CUMPLIMIENTO

- **LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

ESCRITORIO LIMPIO:

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).
- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales en general.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).

- El grupo de Sistemas y TICs podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

USO ADECUADO DE CORREO ELECTRÓNICO:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina/grupo de tecnología podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

USO DE USUARIOS Y CONTRASEÑAS:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

5. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR, definirá un "**Plan de Comunicación en Seguridad de la Información"** a través de su oficina de comunicación interna y externa y el Grupo de Sistemas y TICs, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

CAPACITACIONES EN SEGURIDAD

LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de

seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR.**

7. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c. El Grupo de Sistemas y TICs será el encargado de recopilar y entregar a la Oficina de Control Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TICs será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las politicas.

Elaborado por	Revisado por	Aprobado por
Nombre y Cargo		
MAURICIO GARCES ORDÓÑEZ Profesional Especializado de Sistemas y TICs	**YOHASKY FIORELLA CABALLERO OSPINO** Profesional de Apoyo SGAP. SIG-C	**WILMEN JOSE VASQUEZ**– Coord. GIT para la Gestión del Área de Sistemas y TICS. **MÓNICA INÉS GONZÁLEZ THOMAS** Subdirectora General Área Planeación (e)