POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS

PCE-PL-1

ELABORÓ	REVISÓ	APROBÓ
Cargo: Oficial de Seguridad de la Información **Fecha:** marzo de 2023	**Cargo:** Director SIG **Fecha:** marzo de 2023 **REVISÓ** **Cargo:** Gerente de Proyecto Junior CEAS **Fecha:** marzo de 2023	**Cargo:** Director Sicov **Fecha:** marzo de 2023

TABLA DE CONTENIDO

1. OBJETIVO 3

2. ALCANCE 4

3. REQUISITOS LEGALES Y/O REGLAMENTARIOS 4

4. DEFINICIONES 5

5. POLITICAS 7

5.1. Política general de Seguridad de la información 7

5.2. Organización de la seguridad de la información 8
5.2.1. Actores del SGSI 8
5.2.2. Roles y Responsabilidades 8
5.2.3. Dispositivos móviles 9
5.2.4. Teletrabajo 9

5.3. Seguridad de recursos humanos 10
5.3.1. Antes de asumir el empleo 10
5.3.2. Durante la ejecución del empleo 11

5.4. Gestión de activos 12

5.5. Control de acceso 12
5.5.1. Requerimiento para el control de acceso 12
5.5.2. Gestión de acceso del usuario 13
5.5.3. Responsabilidades del usuario 14
5.5.4. Control de acceso a sistemas y aplicaciones 15

5.6. Criptografía 16
5.6.1. Uso de Controles Criptográficos 17
5.6.2. Funciones y Responsabilidades de Cifrado 17

5.7. Seguridad física y ambiental 17
5.7.1. Áreas seguras 17
5.7.2. Equipamiento 18
5.7.3. Políticas de escritorio limpio y pantalla clara. 20

5.8. Seguridad de las operaciones 20
5.8.1. Procedimientos y responsabilidad de operación 20
5.8.2. Protección contra Malware 21
5.8.3. Copias de seguridad 21
5.8.4. Registro y Seguimiento 22
5.8.5. Gestión de vulnerabilidades técnicas 22

5.9. Seguridad de las Comunicaciones 23
5.9.1. Gestión de seguridad en la red 23
5.9.2. Transferencia de Información 23

5.10. Adquisiciones, desarrollo y mantenimiento de sistemas 24
5.10.1. Requerimientos de seguridad de los sistemas de información 24
5.10.2. Seguridad en los procesos de desarrollo y soporte 25

5.11. Relaciones con proveedores 26
5.11.1. Seguridad de la Información en las Relaciones con los Proveedores. 26
5.11.2. Tratamiento de Seguridad dentro de los Acuerdos con Proveedores 26
5.11.3. Cadena de Suministro de Tecnología de Información y Comunicación 26

5.12. Gestión de incidentes en la seguridad de la información 27
5.12.1. Responsabilidades y Procedimientos 27
5.12.2. Reporte de Eventos de Seguridad de la Información 27
5.12.3. Reporte de Vulnerabilidades de Seguridad de la Información 27
5.12.4. Evaluación de Eventos de Seguridad de la Información y Decisiones sobre los Mismos 27
5.12.5. Respuesta a Incidentes de Seguridad de la Información 27
5.12.6. Aprendizaje Obtenido de los Incidentes de Seguridad de la Información ... 28
5.12.7. Recolección de Evidencia 28

5.13. Cumplimiento 28
5.13.1. Cumplimiento de Requisitos Legales y Contractuales 28
5.13.2. Revisiones de Seguridad de la información 29

6. PRIVACIDAD Y CONFIDENCIALIDAD 29

7. PROPIEDAD INTELECTUAL E INDUSTRIAL 30

8. CUMPLIMIENTO 30

9. REVISIÓN 30

CONTROL DE CAMBIOS

VERSIÓN	FECHA APROBACIÓN	CARGO	CRITERIO(S)	CAMBIO
2	3/03/2023	Director SICOV	Todos	Se ajustan los numerales existentes y se incluyen varios aspectos nuevos en la política.

1. OBJETIVO

Establecer los lineamientos, reglas y directrices de seguridad de la información que plantea el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS y presentar en forma clara y concisa los elementos que conforman la política de seguridad que deben conocer, acatar y dar obligatorio cumplimiento todos los Centros de Enseñanza Automovilística CEAS, con el fin de proteger adecuadamente los activos de información del Sistema de Control y Vigilancia administrados por el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS.

2. ALCANCE

El presente documento es aplicable a todos los procesos administrativos y de control que deben ser cumplidos por los funcionarios activos de los Centros de Enseñanza Automovilística CEAS vinculados con el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, para lograr un alto nivel en cuanto a la protección de las características de calidad y seguridad de la información, aportando con su interacción en la toma de medidas preventivas y correctivas, que representan la finalidad de este escrito. Los usuarios/funcionarios de los CEAS tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS.

3. REQUISITOS LEGALES Y/O REGLAMENTARIOS

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se obliga a prestar los servicios de implementación y operación de la solución tecnológica del Sistema de Control y Vigilancia en los Centros de Enseñanza Automovilística CEA en Colombia, de conformidad con la normativa expedida por la Superintendencia de Puertos y Transporte, mediante Resolución N°. 05790 de 2016, por la cual se reglamentan las características técnicas del sistema de Control y Vigilancia de los Centros de Enseñanza Automovilístico CEA y la Resolución N°. 60832 de 2016, por el cual se expidió el Anexo Técnico para la implementación de los Sistemas de Control y Vigilancia ordenado a través de la Resolución N°. 05790 de 2016.

Resolución 45776 del 19 de septiembre de 2017. Por medio de la cual se autoriza al CONSORCIO SISTEMA INTEGRADO DE GESTION Y SEGURIDAD CEAS-CIAS conformado por las empresas COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN S.A -CI2-, con Nit No. 830.056.140-0 y GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A -GSE S.A., como proveedor de los Sistemas de Control y Vigilancia de los Centros de Enseñanza Automovilística (CEA's).

Ley 769 del 06 de julio de 2002. Por la cual se expide el Código Nacional de Tránsito Terrestre y se dictan otras disposiciones.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
Resolución 5790 del 12 de febrero de 2016. Por la cual se reglamentan las características técnicas del Sistema de Control y Vigilancia de los Centros de Enseñanza Automovilística -CEA y de los Centros Integrales de Atención -CIA.

Resolución 60832 del 04 de noviembre de 2016. Por la cual se expide al anexo técnico para la

implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016.

Decreto 1500 de 2009. Por el cual se establecen los requisitos para la constitución, funcionamiento y habilitación de los Centros de Enseñanza Automovilística, se determina su clasificación y se dictan otras disposiciones.

Resolución 3245 del 21 de julio de 2009. Por la cual se reglamenta el Decreto 1500 de 2009 y se establecen requisitos para la habilitación de los Centros de Enseñanza Automovilística.

Resolución 993 del 25 de abril de 2017. Por la cual se determinan los valores que por cada servicio que prestan los organismos de apoyo deben transferirse al Fondo Nacional de Seguridad Vial y se dictan otras disposiciones.

4. DEFINICIONES

Acceso: Es el privilegio que se le brinda a los funcionarios a las aplicaciones, plataforma y otros recursos tecnológicos, para cumplir con las funciones del cargo.

Activo de Información: Cualquier bien (humano, tecnológico, software, documental o de infraestructura) que tiene valor para la organización y soporta uno o más procesos de negocios y, en consecuencia, debe ser protegido.

Amenaza: Causa potencial de un incidente no deseado, que puede causar daño a los sistemas de información.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y causas de riesgo, estimar la probabilidad e impacto de riesgo, así como evaluar los controles a aplicar para mitigar, transferir, evitar o aceptar el riesgo.

Aplicación: Conjunto de programas desarrollados en diferentes lenguajes de programación orientados a facilitar la administración de la información dentro de un proceso productivo o administrativo de una organización.

Aviso de privacidad: Comunicación verbal y/o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Backup: Copia o respaldo de la información.

Base de datos: Conjunto de registros de datos interrelacionados lógica y/o físicamente, que contienen información de usuario. Conjunto organizado de datos personales que sea objeto de tratamiento.

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que solo pueda leerlo la persona que disponga de la clave de cifrado adecuada para decodificarlo.

Clientes: Personas o entidades que establecen relaciones directas o indirectas con una organización.

Código malicioso: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado.

Confiabilidad: Garantía que la información es la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

Confidencialidad: Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

Control: Medios y acciones para gestionar y mitigar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cumplimiento: Tiene que ver con llevar a efecto las leyes, regulaciones y obligaciones contractuales a las cuales está sujeto el proceso del negocio, es decir, los criterios del negocio impuestos externamente por clientes o entes reguladores.

Custodios de la información: Son los individuos a los cuales se les delegan las labores rutinarias de administración y mantenimiento de los activos de información. Este se debe encargar de aplicar controles para mitigar riesgos existentes sobre los activos y mantener su adecuado funcionamiento. Implementa las políticas y guías fijadas por el propietario o por el ente de control.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y datos biométricos.
Derechos de propiedad intelectual: Los derechos de propiedad intelectual incluyen derechos de copia de software o de documentos, derechos de diseño, marcas registradas, patentes y licencias de código fuente.

Disponibilidad: Es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

Evento de Seguridad de la Información: Es una ocurrencia identificada de un estado en un sistema, servicio o red que indica una posible brecha de seguridad de la información, de las políticas, una falla de los controles o una situación previa desconocida que puede ser relevante a la seguridad.

Integridad: Es la propiedad que busca proteger que se modifiquen la información de forma no autorizada.

Información: Es un grupo de datos supervisados y ordenados, que sirven para construir un mensaje. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Incidente de Seguridad de la Información: Uno o varios eventos de seguridad de la información no deseados o inesperados que tiene una probabilidad significativa de comprometer las operaciones del negocio y por ende amenaza la seguridad de la información.

Plataforma tecnológica: Conjunto de elementos de hardware, software y comunicaciones destinados a un procesamiento de información con características específicas.

Política: Toda intención y directriz expresada formalmente por una organización.

Privado: Información de uso exclusivo de una persona o de la entidad.

Propietario del Activo: Individuo, entidad o unidad de la organización responsable de la administración y control del activo de información.

Riesgo: Posibilidad de que una amenaza pueda explotar una o más vulnerabilidades de un activo o grupo de activo para causar una pérdida o daño de la información.

Seguridad de la información: Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información, al mantener y preservar la confidencialidad, integridad y disponibilidad de la información.

Tercero(s): Cualquier persona natural o jurídica en calidad de proveedor, outsourcing o consultor.

Usuario: Nombre que se asigna al personal (Directo/Temporal) y terceros para poder identificarlos dentro de las diferentes aplicaciones, recursos tecnológicos, etc.

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

5. POLITICAS

5.1. Política general de Seguridad de la información

Para EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS , la información es catalogada como uno de los activos fundamentales y estratégicos para la prestación de los servicios y la toma de decisiones eficientes; por lo cual la Compañía está comprometida con el adecuado cuidado y gestión de la información propia y de los clientes mediante la adopción y aplicación de marcos regulatorios, alineado con las mejores prácticas o estándares internacionales de seguridad de la información y de ciberseguridad, encaminando sus esfuerzos en pro del mantenimiento de la Confidencialidad, Integridad y Disponibilidad de sus activos de información.

La Junta Directiva y la Alta Dirección mediante la aprobación de esta Política declaran su posición y compromiso con el cumplimiento de los requisitos definidos en el marco del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, aspectos en los cuales se involucra directamente la función de seguridad de la información y ciberseguridad, que tiene como propósito principal mantener un ambiente razonablemente seguro, alineado a la misión, objetivos estratégicos de EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS y requerimientos regulatorios aplicables, definiendo e implementando buenas

prácticas que permitan minimizar posibles impactos no deseados que puedan comprometer los principios esenciales de la seguridad de la información.

Para EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS las acciones o toma de decisiones alrededor del SGSI estarán determinadas en pro de alcanzar las siguientes premisas:

- Minimizar el riesgo en las funciones de EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS con un enfoque de priorización basado en riesgos.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios determinados en la política de imparcialidad y no discriminación.
- Cumplir con los principios establecidos en manual del programa de transparencia y ética empresarial PTEE en materia de confidencialidad de información.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores, terceros, practicantes y clientes de EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS
- Garantizar la continuidad del negocio frente a incidentes.

5.2. Organización de la seguridad de la información

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS define un marco de referencia para gestionar y controlar la implementación y operación de seguridad de la información a nivel interno.

La estructura del Sistema de Gestión de Seguridad de la Información en EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, se encuentra alineada con los requerimientos y disposiciones de los planes estratégicos.

5.2.1. Actores del SGSI

- Comité de Seguridad de la Información y Gestión del Riesgo.
- Directores de Área.
- Dueños de los procesos misionales y operativos del negocio.
- Oficial de Seguridad.
- Colaboradores.
- Clientes.
- Órganos de Control.
- Proveedores

5.2.2. Roles y Responsabilidades

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS define, estructura, establece y designa los roles y responsabilidades de seguridad de la información para todas las direcciones, los cuales se estipulan en el perfil y funciones del cargo; por lo tanto, es responsabilidad del Director del Capital Humano mantener y actualizar el perfil de cada cargo en este sentido.

Los funcionarios y terceros deben conocer sus roles y responsabilidades y deben ejecutar sus funciones acordes a su rol y a su responsabilidad dentro del SGSI.

Sin perjuicio de la Estructura Organizacional definida a continuación, toda la organización es responsable de la gestión y administración de la seguridad de la información.

5.2.3. Dispositivos móviles

El CONSORCIO asigna y permite el uso de dispositivos móviles de conexión inalámbrica, únicamente al interior de las instalaciones del Centro de Enseñanza, exclusivamente para desarrollar y cumplir con los objetivos laborares pactados en el contrato de vinculación, por tanto, el CEA deberá garantizar que no se almacene en estos dispositivos información personal o cualquiera que no competa con la operatividad del CEA.

Los dispositivos móviles asignados al CEA, son de propiedad del CONSORCIO, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.

El CEA acepta que, los medios de almacenamiento de los dispositivos celulares pueden ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por EL CONSORCIO, con el fin de establecer un cerco de seguridad a la información que en ellos se administre.

El CEA debe garantizar que los dispositivos que no hagan parte del KIT inicial de CEAS, no podrán conectarse a la red que hace parte de la IP Pública Fija que fue registrada y autorizada en el momento de la habilitación del CEA.

El CEA está en la obligación de reportar cualquier anomalía en el funcionamiento de los dispositivos móviles al CONSORCIO, ya sea a nivel de software o de sus componentes físicos. Las solicitudes de verificación del funcionamiento de dichos dispositivos se realizarán por medio de la mesa de ayuda del Sistema de Control y Vigilancia AULAPP, a través de ticket al correo mesadeservicios@seguridadcea.com.

5.2.4. Teletrabajo

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS o cualquiera de sus partes, dispone de herramientas que garantizan el uso adecuado de las políticas y medidas de seguridad para proteger la información que se accede, procesa y almacena a través del uso de trabajo remoto.

El Oficial de Seguridad de la Información debe establecer los controles que tendrá el personal que actúe en modalidad de trabajo remoto.

Los funcionarios que operen bajo la modalidad de trabajo remoto tienen en los dispositivos que les asigna la compañía un antivirus corporativo instalado de forma adecuada con los bloqueos necesarios para garantizar la seguridad de la información fuera del ambiente de la oficina.

5.3. Seguridad de recursos humanos

5.3.1. Antes de asumir el empleo

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS asegura que los aspirantes a los cargos que harán parte del mismo, son los adecuados para los roles y responsabilidades que van a desempeñar, de acuerdo con lo establecido en el Procedimiento de Atracción y Selección de Personal.

Selección del Personal

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS verifica todos los antecedentes de todas las personas que aspiren a cargos, empleos o vacantes disponibles, de acuerdo con la legislación, normas, ética, requisitos del negocio, clasificación de la información, accesos a sistemas de información y riesgos asociados a los mismos.

El Director del área o proceso de Capital Humano de cada una de las partes del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS debe garantizar que se realiza la revisión de todos los antecedentes disciplinarios, penales y referencias de los candidatos que apliquen a la compañía.

Los aspirantes a un cargo en EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, deben entregar la totalidad de la información solicitada de forma verídica de las referencias personales y profesionales.

Términos y Condiciones del Empleo

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS o cualquiera de sus partes, deberá establecer un contrato con todo empleado o tercero que tenga algún tipo de relación contractual con EL CONSORCIO, en el cual se definen todas las responsabilidades de estos frente a seguridad de la información, dicho contrato deberá incluir las cláusulas de confidencialidad, protección de datos y entrega de información con los terceros.

El Oficial de Seguridad de la Información podrá revisar el nivel de acceso a la información a la que tenga cada empleado según el rol que le corresponda dentro de la organización.

Acuerdos de confidencialidad

En EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS todos los funcionarios y terceros que tengan acceso a la información de la unidad de gestión, deben firmar un acuerdo de confidencialidad y buen manejo de la información, para que se asegure que la información no sea publicada o conocida por personal no autorizado. Quienes incumplan estos acuerdos o compromisos de confidencialidad podrán ser sancionados de acuerdo con el régimen disciplinario, establecido al interior de cada una de las partes del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, sin

perjuicio de las reclamaciones judiciales y/o extrajudiciales que sean pertinentes.

5.3.2. Durante la ejecución del empleo

La Dirección del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS debe asegurar que los funcionarios y terceros tomen conciencia y cumplan las responsabilidades de seguridad de la información.

Responsabilidades de la dirección

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS exige a los funcionarios y terceros el cumplimiento de las políticas y procedimientos de seguridad de la información establecidos, según lo establecido en los contratos de trabajo y demás documentos asociados.

Desde la dirección del CONSORCIO se debe exigir a todos los niveles del mismo, el cumplimiento de las políticas a los funcionarios y terceras partes según se establece en los acuerdos contractuales.

Toma de conciencia, educación y formación en Seguridad de la Información

Todos los colaboradores de EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS y terceros deben ser sensibilizados y capacitados en toma de conciencia, políticas y procedimientos de seguridad de la información pertinente, y en sus actualizaciones, de acuerdo con las necesidades, funciones y roles asumidos en la organización.

Todos los colaboradores deben tomar los cursos de sensibilización y capacitación que organice el CONSORCIO y aprobar los exámenes que se realicen dentro de los mismos en los tiempos establecidos para tal fin.

Las formaciones y sensibilizaciones deberán quedar estipuladas en un Plan de formación, el seguimiento para el cumplimiento y la eficacia deberá ser gestionada por Capital Humano.

El Oficial de Seguridad de la Información cuando aplique realiza la formación y sensibilización para funcionarios y terceros, en todo lo relacionado con seguridad de la información.

Proceso Disciplinario

EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS a través de Capital Humano, asegura el cumplimiento del Reglamento Interno de Trabajo, como medida de control disciplinaria en la organización en caso de violaciones o infracciones relacionadas con la seguridad de la información por parte de funcionarios, sobre los cuales aplican dichas medidas.

La dirección del CONSORCIO realiza el proceso adecuado con los proveedores y terceros que incumplan con las políticas de seguridad de la información.

Terminación y cambio de responsabilidades de empleo o labor contratada

La dirección del CONSORCIO con el apoyo del Oficial de Seguridad de la Información define, comunica y vela por el cumplimiento de las responsabilidades y deberes de seguridad de la información que permanecen válidos para los funcionarios y terceros después de la terminación del contrato laboral o cambio de cargo.

Capital Humano reportará los cambios de cargo que se presenten, el Oficial de Seguridad debe revisar los nuevos accesos y solicitar la depuración y el ajuste de permisos al área de Infraestructura.

5.4. Gestión de activos

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS es el dueño de la propiedad intelectual del Sistema de Control y Vigilancia denominado Aulapp, de las versiones y actualizaciones a que den lugar en cumplimiento de la Resolución 45776 del 19 de septiembre de 2017.
El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS es propietario y administrador de los activos de información (Plataforma Tecnológica Aulapp Web, Apps móviles y equipos: escáner, pad de firmas, cámara web, lectores biométricos, hub multipuertos, celulares, validadores vehiculares). En tanto, los CEA serán responsables del cuidado, la correcta manipulación y el buen uso de los equipos anteriormente mencionados, así mismo, los funcionarios vinculados a los CEA cuyos usuarios se encuentren activos en la Plataforma Tecnológica Aulapp tienen la obligación de conocer la información de los procesos asociados a sus roles, con respecto a su interacción con la Plataforma Web y Aulapp móviles, con el fin de garantizar la correcta operatividad del Sistema en los CEA.
El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por su Sistema de Control y Vigilancia Aulapp y se reserva el derecho de conceder el acceso a la información.

Por su parte, los CENTROS DE ENSEÑANZA AUTOMOVILÍSTICA CEAS deben clasificar y monitorear sus activos de información, tales como, bases de datos, archivos físicos, sistemas de información, cableado, redes, dispositivos de almacenamiento e incluso los mismos funcionarios que manejan datos o conocimiento específico de la operación propia del CEA, con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir e implementar los niveles de protección y medidas de tratamiento, evaluando las tres características de la información en las cuales se basa la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

5.5. Control de acceso

5.5.1. Requerimiento para el control de acceso

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, define como mínimo las siguientes reglas a implementar por los CEA, con el fin de asegurar un acceso controlado al Sistema de Control y Vigilancia AULAPP. El control de acceso al Sistema AULAPP se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas. El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil de usuario asignado.

5.5.2. Gestión de acceso del usuario

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se asegurará el acceso de los usuarios autorizados y autenticados a las plataformas de la siguiente manera:

Registro y cancelación del registro de usuarios.

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS por medio del Sistema de Control y Vigilancia SICOV AULAPP controlará el registro de nuevos usuarios mediante las herramientas de Gestión Documental dispuestas por la Plataforma Tecnológica AULAPP. En cuanto a la cancelación de los usuarios del CEA y su interacción con los sistemas y servicios de información, las novedades deberán ser reportadas por el Representante Legal del CEA mediante radicación de ticket.

El personal interno de EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS y los usuarios de los CEA no deberá compartir sus usuarios con otras personas internas o externas durante la existencia del mismo usuario.

El personal externo del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, ni personal externo de los CEA, tendrán usuarios dentro del Sistema de Control y Vigilancia SICOV AULAPP.

Es deber de los CEAS reportar las novedades referentes al estado de vinculación de sus usuarios, por lo tanto, deberán solicitar la deshabilitación de los mismos mediante radicación de ticket a mesadeservicios@seguridadcea.com.

Creación de usuarios especiales.

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS podrá generar, para sus colaboradores internos, usuarios especiales cuyas características difieran de las normalmente definidas para usuarios finales.

Dichos usuarios especiales se definirán con el objetivo de atender aspectos tales como la gestión de aplicativos, propietarios de esquema en base de datos, o a nivel de red, usuarios específicos de área de acuerdo con la gestión requerida y aprobada. Los mismos serán monitoreados de forma automática, y sus acciones serán reportadas al Oficial de Seguridad de la Información.

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS no asignará usuarios especiales a los CEAS ni a sus colaboradores.

La Dirección General autorizará y solicitará la creación de estos usuarios especiales según sea el caso.

Aparte de las autorizaciones que asigne la Dirección General, ningún funcionario o tercero tendrá usuarios especiales.

Suministro de Acceso de Usuarios

Los responsables de los sistemas de información deben suministrar, asignar o revocar de manera formal los derechos de acceso de los usuarios a los sistemas y servicios de información cuando

sea necesario.

El Líder Técnico de la Plataforma Tecnológica AULAPP deberá asignar o deshabilitar los usuarios según se reporte por parte de los Supervisores de Mesa de Ayuda.

Gestión de Derechos de Acceso Privilegiado

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se restringirá y controlará la asignación y uso de los derechos de acceso privilegiado a los sistemas de información.

Es deber de los funcionarios que cuenten con accesos privilegiados no deberán realizar ningún cambio que afecte la integridad de la Plataforma Tecnológica AULAPP.

Gestión de Información de Autenticación Secreta de Usuarios

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se controlará la asignación de información de autenticación secreta.

Los usuarios que reciban su contraseña por correo electrónico deberán realizar el cambio de contraseña de manera inmediata, por solicitud del sistema informático, utilizando contraseñas con las restricciones establecidas en el presente documento.

En caso de olvido de la información de Autenticación, el usuario deberá realizar el restablecimiento de las credenciales directamente en la Plataforma Tecnológica AULAPP.

Revisión de los Derechos de Acceso de Usuarios

El líder Técnico de la Plataforma Tecnológica AULAPP estará encargado de la revisión de los derechos de acceso a los usuarios y los funcionarios deberán tener derechos de acceso bajo mínimo privilegio según las funciones de su cargo.

Retiro o Ajuste de los Derechos de Accesos

Los derechos de acceso de los funcionarios y terceros (Proveedores, Contratistas o Pasantes), a la información y los sistemas de información del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS deben ser retirados inmediatamente, de forma total o parcial, en caso de hacer terminado su contrato laboral, acuerdo o en caso de cambio de funciones o del cargo, se inactivarán con paz y salvo de los trabajadores desvinculados de la empresa.

El CEA no deberá solicitar los usuarios de funcionarios ya retirados, sino que deberá crear un nuevo perfil según lo requiera.

5.5.3. Responsabilidades del usuario

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS exigirá y pedirá cuentas a los usuarios de sistemas de información sobre el cumplimiento de las políticas de seguridad establecidas.

Uso de Información de Autenticación Secreta

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se exigirá a funcionarios y a los CEAS el cumplimiento de las buenas prácticas sobre el uso de la información de autenticación secreta (Nombres de Usuario y Contraseñas), para el ingreso a los sistemas de información.

Los usuarios deberán utilizar claves que cumplan con las siguientes características:

- Claves de 8 o más caracteres
- No repetir las ultimas 5 claves
- Las claves deberán contener como mínimo: Letra Mayúscula, Minúscula, números y caracteres especiales.

Los usuarios deberán cambiar sus contraseñas cada 60 días y es deber del Ingeniero de Infraestructura implementar dicho control dentro del directorio activo.

La Plataforma Tecnológica enviará las credenciales de primer acceso al Representante Legal del CEA con la parametrización de exigir el cambio de clave después de la primera validación.

Es deber del Oficial de Seguridad de la Información solicitar el cambio de credenciales de correo de un usuario puntual en el caso en el que se encuentre que dicha cuenta fue comprometida en un ataque hacia otro sitio.

Las contraseñas de los diferentes usuarios de la Plataforma Tecnológica AULAPP se almacenan de forma cifrada y en ninguna circunstancia se podrán almacenar en texto plano.

Los funcionarios de los CEAS no deberán compartir sus claves con cualquier otra persona de forma interna o externa ni deberán anotarla en cualquier documento físico o electrónico.

5.5.4. Control de acceso a sistemas y aplicaciones

Los propietarios y responsables de los activos de información deben evitar el acceso no autorizado a la Plataforma Tecnológica AULAPP.

Restricción de Acceso a la Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, el acceso a la información y sistemas de información será restringido de acuerdo con las políticas de control de acceso establecidas por EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS.

Ningún funcionario de los CEA podrá acceder a la información a la cual no tenga acceso ni deba tener acceso, en caso de tener dicho acceso deberá reportar el caso a la mesa de ayuda a través del correo electrónico mesadeservicios@seguridadcea.com solicitando el respectivo bloqueo de acceso sobre el mismo.

Ingreso Seguro

El acceso a los sistemas de información del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS será controlado, por medio de sistemas de autenticación.

Sistemas de Gestión de Contraseñas
La asignación temporal de las contraseñas a los usuarios de los CEAS se realiza exclusivamente por el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS. Los usuarios de los CEAS deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y, por lo tanto, se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, enviará una contraseña temporal al correo electrónico con el cual fue registrado el usuario/funcionario del CEA, quien, a su vez, deberá ingresar a dicho correo electrónico y con ayuda la contraseña temporal, realizar el cambio y asignación de una contraseña personal para el acceso al Sistema de Control y Vigilancia AULAPP.

- Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
- Las contraseñas no deberán ser reveladas.
- Las contraseñas no se deberán escribir en ningún medio.
- Los funcionarios deben digitar siempre su usuario y contraseña para acceder al Sistema de Control y Vigilancia AULAPP.
- Las contraseñas no se deben guardar de forma automática en los inicios de sesión de las aplicaciones para acceder al Sistema de Control y Vigilancia AULAPP.
- Es deber de cualquier funcionario activo de los CEAS reportar cualquier sospecha de que una persona no autorizada esté utilizando una contraseña o un usuario que no le pertenece.

Uso de Programas Utilitarios Privilegiados

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS restringirá y controlará estrictamente el uso de programas utilitarios para todos los colaboradores del CONSORCIO, excepto para aquellos autorizados que tengan perfil de administrador.

Los colaboradores del CONSORCIO deberán tener instalados únicamente los programas autorizados con los permisos necesarios para su ejecución únicamente.

Control de Acceso a Códigos Fuente de Programas

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS restringirá el acceso a los códigos fuente de los programas o desarrollos que hacen parte de las operaciones del negocio.

Los terceros que la Dirección del CONSORCIO determine que deban desarrollar soluciones para la compañía deberán dar acceso al código fuente únicamente al personal que requiera trabajar en el desarrollo de sus funciones.

5.6. Criptografía

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS asegurará el uso apropiado y eficaz de la criptografía en sus operaciones con el fin de proteger la confidencialidad, autenticidad e integridad de la información.

5.6.1. Uso de Controles Criptográficos

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS implementará cifrados seguros con los controles adecuados que permitan proteger la información en las operaciones del negocio.

La Plataforma Tecnológica AULAPP deberá tener certificado digital SSL con criptografía apropiada y fuerte con la finalidad de reducir el riesgo de que los clientes y usuarios lleguen a sufrir ataques de DNS y sean redirigidos a páginas falsas. Los servicios del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS públicos deberán ser accedidos de forma segura por medio de certificados digitales, de lo contrario deberán ser accedidos por medio de VPN para el caso de servicios que por necesidad de negocio no puedan asegurarse con certificado digital (HTTP, FTP, entre otros).

Las credenciales de acceso a los distintos sistemas del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se almacenan de forma segura utilizando criptografía de una sola vía que no esté rota y que cuente con sistemas de SALT que permitan la diferenciación de dos credenciales iguales dentro de las bases de datos del sistema.

Los clientes u organizaciones que requieran consumir servicios del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS deberán realizarlo por medio de enlaces dedicados, VPN o por medio de SSL únicamente, por bloqueo a nivel de seguridad perimetral permitiendo únicamente las fuentes y los servicios a consumir, no se autorizarán consumos por otros medios salvo que los mismos tengan un nivel criptográfico adecuado para la ejecución de actividades. (AES256-SHA256)

5.6.2. Funciones y Responsabilidades de Cifrado

Todos los CEA y colaboradores serán responsables de cumplir las políticas de cifrado de la información en toda transmisión de información secreta, confidencial o privada.

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS utiliza técnicas criptográficas como mecanismo de protección de la información en los siguientes casos:

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS cifra las unidades de almacenamiento de equipos portátiles de los colaboradores del CONSORCIO, salvaguardando la confidencialidad e integridad de la información.

La información confidencial y reservada que se transmite cifrada a las partes interesadas pertinentes del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, según lo establecido en la Política de Transferencia de la Información.

Las aplicaciones web utilizadas en el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS utilizan certificado SSL.

5.7. Seguridad física y ambiental

5.7.1. Áreas seguras

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS

se previene el acceso físico no autorizado, daño e interferencia de su información en sus instalaciones y áreas de procesamiento de información a través de controles de accesos biométricos.

Los funcionarios y terceros no deberán acceder a las áreas seguras de la compañía a menos que por perfil de cargo no estén autorizados para el desarrollo de sus funciones.

5.7.2. Equipamiento

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS prevendrá la pérdida, daño, robo o compromiso de los activos de información e interrupción de las operaciones de su negocio.

- Los CEA deberán garantizar que, los equipos de cómputo destinados para realizar cotejos biométricos contra la Registraduría Nacional del Estado Civil RNEC, cuenten con Sistema Operativo licenciado.

- Los CEA deberán garantizar que, los equipos de cómputo destinados para realizar cotejos biométricos contra la Registraduría Nacional del Estado Civil RNEC, cuenten con Antivirus licenciado e instalado, dicho antivirus deber ser de tipo comercial y el CEA deberá garantizar que su licencia se extienda hasta la finalización del contrato con el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS.
- Los CEA deberán contar con el complemento Firmware del proveedor de huelleros actualizado a la versión más reciente (FIRMWARE NEMO V05.01 CBM with FFD), de no contar con dicha herramienta, deberá solicitar su instalación a la Mesa de Ayuda, a través de ticket mediante el correo electrónico mesadeservicios@seguridadcea.com

Ubicación y Protección de los Equipos
Los equipos de los colaboradores del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, están ubicados y protegidos contra amenazas, peligros del entorno y acceso no autorizado.

Servicios de Suministro
Los equipos de los colaboradores del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, estarán protegidos contra falla o interrupción causada en el suministro de los servicios eléctricos, comunicaciones, administrativos o cualquiera que sea necesario para la continuidad del negocio.

Del Procesamiento de la Información
El procesamiento a la información que se realice sobre cualquier componente de la plataforma tecnológica debe cumplir con la normatividad establecida en materia de seguridad de la información con el fin de preservar la confidencialidad, integridad y disponibilidad de esta.

Seguridad del Cableado
Todo el cableado de energía eléctrica, telecomunicaciones y servicios de suministro de la infraestructura interna del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, está adecuadamente organizado y asegurado contra amenazas, interceptación o daños.

Los colaboradores del CONSORCIO deberán cuidar los elementos eléctricos y de red a los que

tienen acceso a nivel de cableado, y deberán reportar de forma inmediata cualquier anomalía del cableado que pueda afectar el funcionamiento adecuado de la labor de los funcionarios de la compañía.

Mantenimiento de Equipos y Software
El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS realizará mantenimiento periódico a los equipos de cómputo de sus colaboradores de acuerdo con las características y recomendaciones del fabricante o cuando sea requerido por eventos o incidentes presentados, con el fin de asegurar la continuidad en su funcionamiento, integridad, disponibilidad y conservación de estos.

Los CEAS deberán programar y ejecutar mantenimientos preventivos periódicos, mínimo una vez al año, en pro del funcionamiento correcto de los equipos entregados por el CONSORCIO. Este mantenimiento deberá ser realizado por personal idóneo y certificado para tal fin.

Retiro de Activos
El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS no retirará de sus instalaciones los equipos, información o software sin previa autorización del propietario o responsable del activo de información.

Los CEAS deberán informar sobre el retiro de los activos a la Dirección de CONSORCIO, quien determinará si autoriza el retiro.

En caso de que un CEA termine su relación contractual con el CONSORCIO, deberá devolver los equipos entregados por este a las oficinas del mismo.

Seguridad de equipos fuera de las instalaciones
En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se suministrarán e implementarán medidas de seguridad apropiadas para los equipos entregados a los colaboradores que requieran estar fuera de las instalaciones, contemplando los riesgos a los que se pueden ver expuestos. Los funcionarios deberán tener el antivirus instalado con las políticas de bloqueo y de seguridad implementadas y las unidades de almacenamiento debidamente cifradas.

Los CEAS no están autorizados en ninguna circunstancia a retirar de sus instalaciones los equipos entregados por el CONSORCIO. Si por alguna circunstancia se tuviese la necesidad de retirar los equipos de las instalaciones los CEAS deberán informar sobre el retiro de los activos a la Dirección de CONSORCIO, quien determinará si autoriza el retiro.

Disposición Segura, Reutilización o Eliminación de Equipos
En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS antes de la eliminación, disposición o reutilización de los equipos para ser entregados a funcionarios o terceros se debe verificar todos los elementos que lo componen, especialmente los medios de almacenamiento (discos, memorias, unidades ópticas, entre otros), con el fin de asegurar que toda información y/o software licenciado haya sido retirado o sobrescrito de forma segura.

Equipos de Usuario Desatendido

Todos los CEAS y funcionarios del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS son responsables de asegurar que los equipos desatendidos cumplen con la protección adecuada. Así mismo, los CEA deberá establecer un bloqueo automático por inactividad para todas las estaciones de trabajo, este tiempo deberá ser máximo de cinco (5) minutos, y sólo se podrá desbloquear únicamente con la contraseña del usuario.

Los CEAS y funcionarios del CONSORCIO deberán bloquear su equipo cada vez que se retiren de su escritorio.

Limitación del tiempo de conexión

La Plataforma Tecnológica AULAPP está configurada para que al detectar un tiempo de inactividad de cinco (5) minutos se cierre la sesión.

5.7.3. Políticas de escritorio limpio y pantalla clara.

El CEA debe garantizar que:

- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los funcionarios bloqueen su estación y sólo se podrá desbloquear con el usuario y la contraseña del usuario.

- Establecer un tiempo mínimo (que no supere cinco -5- minutos) para que todas las estaciones de trabajo se bloqueen automáticamente por inactividad y sólo se podrá desbloquear únicamente con la contraseña del usuario.

- Garantizar que la autenticación de usuario sea requerida, cada vez que el equipo de cómputo se encienda, reinicie o bloquee.

5.8. Seguridad de las operaciones

5.8.1. Procedimientos y responsabilidad de operación

En relación a los procesos administrativos del CEA, como lo son manejo de personal, contratos vinculación, términos, etc., el CONSORCIO no toma decisiones, ni asume ningún tipo de responsabilidad en cuanto a las decisiones y aprobaciones que adopte el CEA, ni sobre resultados de estudios, encuestas, niveles de satisfacción de empleados y de los realizados a usuarios del CEA, puesto que el CONSORCIO se limita a verificar información y transmitirla por los canales establecidos para ello, en consecuencia, estas decisiones corren por cuentan exclusiva del CEA. Así mismo, el CEA acepta que el CONSORCIO no se responsabiliza por las decisiones que adopte el CEA con base en esa información, ni por riesgos que, de cualquier índole, directa o indirectamente, como consecuencia de las decisiones del CEA pudiesen causarse. Así mismo, no habrá responsabilidad alguna a cargo del CONSORCIO, por la calidad, actualidad y veracidad de la información que le haya sido transmitida por las fuentes, ni en relación con el suministro de información errónea por parte del CEA y/o sus empleados, usuarios, etc.

5.8.2. Protección contra Malware

- Los CEA deberán implementar, ejecutar o poner en marcha, todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información necesarios para estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso al Sistema de Control y Vigilancia AULAPP.
- Los CEA no deberán deshabilitar o desinstalar, sin previa autorización, las herramientas y demás mecanismos de seguridad implementados por el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS. Sin embargo, de ser necesario, los CEA deberán establecer comunicación con la Mesa de Ayuda, a través de correo electrónico mesadeservicios@seguridadcea.com, mediante ticket, donde se dará la gestión debida al caso.
- Los CEA deberán realizar las actualizaciones permanentemente, a las herramientas y demás mecanismos de seguridad según lo disponga el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, con el fin de proteger el ingreso de programas o software malicioso.
- Los CEA no tienen permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de Sistema de Control y Vigilancia AULAPP.
- Los CEAS serán responsables de que sus funcionarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.
- Los CEA deberán inspeccionar, como mínimo una vez por mes, sus sistemas, equipos e información, con el fin de verificar que no haya presencia de código malicioso, que pueda afectar el desempeño de estos y por ende del Sistema de Control y Vigilancia Aulapp

5.8.3. Copias de seguridad

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se protege los activos de información contra la pérdida de datos o información y asegura la integridad, confidencialidad y disponibilidad de esta.

Respaldo de la Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se realizarán copias de seguridad de la información como respaldo o Backup de la misma y se validarán a través de pruebas periódicas de acuerdo con las políticas de respaldo o Backup de la información.

Es deber del equipo de Infraestructura realizar los Backup de los sistemas de información misionales del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS.

Copia de respaldo de información de equipos de colaboradores.
La información de los equipos de desktop y laptop será resguardada en el disco de red, por medio

de Backup específicamente a la carpeta (mis documentos) del equipo del colaborador, cuando el colaborador se retire del CONSORCIO.

Copias de respaldo de información de Base de datos.
La base de datos se respalda con un replicaset de 3 nodos.

Restauración de copias de respaldo
Es deber del equipo de Infraestructura asegurar la integridad de las copias de respaldo, ejecutando pruebas de restauración de manera aleatoria, esta actividad deberá quedar consignada en un cronograma, ejecutada y revisada por quien designe el director del CONSORCIO.

Redundancias.
Se cuenta con medios de almacenamiento, conexiones eléctricas, de procesamiento de datos y comunicación, que incluyan tolerancia a fallos.

5.8.4. Registro y Seguimiento

Registro de eventos

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se elaborarán, conservarán y revisarán de forma permanente los registros de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información presentados en las operaciones del negocio.

Protección de la Información de Registro
En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se protegerán la información de registro y las instalaciones donde se encuentran guardados, contra alteraciones y acceso no autorizado.

Registros del Administrador y del Operador

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se registrarán, protegerán y revisarán cuando se requiera las actividades de administradores y operadores de los sistemas de información.

Sincronización de Relojes

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se mantendrán sincronizados todos los relojes de los sistemas de información de acuerdo con la hora legal Colombiana consultando los servidores NTP autorizados por la compañía.

5.8.5. Gestión de vulnerabilidades técnicas

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se previene y minimiza los riesgos de la explotación de las vulnerabilidades técnicas por usuarios. Por tal motivo, se realizarán pruebas de hacking ético que permitan identificar oportunamente las vulnerabilidades técnicas de los sistemas de información, evaluar la exposición del CONSORCIO

SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS frente a las mismas y aplicar los planes de remediación o medidas adecuadas y necesarias que permitan la mitigación del riesgo en los mismos.

Se realizarán pruebas de hacking ético externas como parte de las políticas y buenas prácticas de seguridad de la información por lo menos una vez al año, cuando se evidencie alguna necesidad manifiesta de realizarlas o cuando sea requerido por la Dirección del CONSORCIO.

5.9. Seguridad de las Comunicaciones

5.9.1. Gestión de seguridad en la red

Los CEA deberán garantizar que las estaciones dispuestas para la validación biométrica contra la Registraduría Nacional del Estado Civil RNEC, cuenten con una conexión a internet cableada. No está autorizada la conectividad mediante WiFi en dichas estaciones.

5.9.2. Transferencia de Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se mantendrá la seguridad de la información que se intercambia interna o externamente con terceros.

Directrices y Procedimientos de Transferencia de Información
En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se controlará la transferencia e intercambio formal de información a través de cualquier tipo de medio o servicio de comunicación.

Los CEA y los colaboradores del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS deberán utilizar canales seguros en la transmisión de su información y deberán mitigar los riesgos de la transferencia manual de la información a fin de garantizar la integridad y disponibilidad de esta.

Acuerdos sobre Transferencia de Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se establecerán acuerdos o convenios a nivel interno y con terceros para la transferencia segura de la información, software o cualquier activo de información respetando la legislación aplicable al caso.

Los CEA y los colaboradores del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS deberán transmitir la información por canales seguros o cifrada según sea el caso y deberán exigir el uso de transmisión segura en todo momento.

Mensajería Electrónica

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se protegerá la información manejada a través de la mensajería electrónica o cualquier medio de correo electrónico y redes sociales.

Los colaboradores del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS podrán ser sometidos a monitoreo constante del correo electrónico por parte del Oficial de Seguridad de la Información y no deberán utilizar el correo electrónico para enviar información sensible a correos personales o de terceros no autorizados, ni deberán usar el correo para fines distintos a los de ejecución de sus funciones.

El correo electrónico asignado por el CONSORCIO, así como los equipos de cómputo o electrónicos que se han asignado para la ejecución de las labores únicamente pueden ser utilizados bajo la finalidad laboral mientras dure el vínculo contractual con EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS y se considerará falta grave el uso de equipo corporativo para fines personales.

- Los colaboradores del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS son responsables de las actividades realizadas con su cuenta de correo corporativo.
- En el caso de recibir un correo electrónico sospechoso, este no debe ser abierto y se debe notificar por medio de correo electrónico al Oficial de Seguridad de la Información de manera inmediata.
- Adjunto en cada correo electrónico se incluye un aviso de confidencialidad, de manejo de datos personales de acuerdo con la ley 1581 del 2012 y 1266 del 2008 de Habeas Data. De igual manera se hace aclaración que las opiniones hechas por los funcionarios del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS son propias y no comprometen de ninguna forma a la compañía.

Acuerdos de Confidencialidad

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se identificarán, documentarán y revisarán periódicamente los acuerdos de confidencialidad, el cual cumpla las necesidades de protección de la información del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, de acuerdo con los requisitos legales, contractuales y buenas prácticas de seguridad de la información vigentes.

Los CEAS deberán cumplir y hacer cumplir los acuerdos de confidencialidad que firmen con el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS o que le apliquen al CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS producto de las relaciones comerciales y contractuales que manejan.

- No se permite el intercambio de información de propiedad del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, de sus clientes y/o de sus funcionarios, con terceros, sin la autorización previa.
- Para los Acuerdos de Confidencialidad o de no divulgación establecidos entre el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS y los CEAS, la Dirección del CONSORCIO realizará una revisión anual, evaluando la pertinencia de estos, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

5.10. Adquisiciones, desarrollo y mantenimiento de sistemas

5.10.1. Requerimientos de seguridad de los sistemas de información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS

la seguridad será parte integral de los sistemas de información durante todo su ciclo de vida el cual incluye requisitos sobre sistemas operativos, infraestructura, aplicaciones y servicios desarrollados o adquiridos para los usuarios y aquellos sistemas de información que prestan servicios a través de redes públicas.

Análisis y Especificación de Requisitos de Seguridad de la Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se incluirán requisitos de seguridad de la información para nuevos, cambios o mejoras en desarrollos o sistemas de información.

Seguridad de Servicios de las Aplicaciones en Redes Públicas

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se trabaja por preservar la seguridad de la información expuesta en servicios web o redes públicas contra amenazas informáticas, incumplimientos contractuales y legales, divulgación o modificaciones no autorizadas.

Los CEAS deberán acceder a la aplicación WEB de la Plataforma Tecnológica AULAPP exclusivamente desde la IP Pública Fija previamente autorizada, utilizando protocolos y puertos seguros cifrados que permitan garantizar la confidencialidad e integridad de la información, así mismo, deberán reportar cualquier falla o cualquier riesgo que se detecte dentro de los servicios web de manera oportuna con la finalidad de prevenir la materialización de los riesgos.

Protección de Transacciones de los Servicios de las Aplicaciones

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se protegerán y validarán las transacciones de servicios de aplicación con el fin de evitar transacciones incompletas, enrutamientos erróneos, alteración de mensajes, divulgación, duplicación o reproducción no autorizadas de mensajes.

Los CEAS deberán utilizar únicamente los canales transaccionales definidos por EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS utilizando y siguiendo las prácticas de seguridad implementadas y solicitadas con la finalidad de garantizar que las transacciones se generan de forma completa y adecuada hasta su destino.

5.10.2. Seguridad en los procesos de desarrollo y soporte

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se deberá solicitar la implementación de seguridad de la información en todo el ciclo de vida de desarrollo de sistemas de información aplicando las siguientes políticas:

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se establecen y aplicarán directrices para el desarrollo, adquisición o alquiler de software, junto con las licencias a las que haya lugar.

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS establece los lineamientos de desarrollo seguro y los deja estipulados en el Manual de Desarrollo Seguro.

5.11. Relaciones con proveedores

5.11.1. Seguridad de la Información en las Relaciones con los Proveedores.

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se protegerán los activos de información accesibles por terceros.

Los proveedores deberán firmar un acuerdo de confidencialidad como requisito en la etapa previa de la contratación, en caso de requerir información reservada o confidencial e igualmente de requerir acceso a áreas seguras críticas del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS.

5.11.2. Tratamiento de Seguridad dentro de los Acuerdos con Proveedores

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se establecerán y acordarán los requisitos de seguridad de la información con los terceros a través de acuerdos de niveles de servicio con el fin de establecer los derechos de acceso, y de procesamiento, almacenamiento, y transmisión de información que da soporte a los procesos misionales de EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS y de sus clientes.

Es deber de las terceras partes dar cumplimiento a la seguridad de la información que establezca el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS en sus políticas como un mínimo posible como acuerdo inicial.

5.11.3. Cadena de Suministro de Tecnología de Información y Comunicación

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS establecerá acuerdos con terceros el cual incluyan los requisitos de seguridad de la información en el suministro de productos de servicios de las tecnologías de la información y las comunicaciones.

Seguimiento y Revisión de los Servicios de los Proveedores

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se podrá monitorear, hacer seguimiento, revisión y auditorías periódicas o cuando se requiera a la prestación de los servicios contratados con terceros.

Gestión de Cambios en los Servicios de los Proveedores

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se controlarán los cambios en los servicios, mantenimiento y mejora de políticas, procedimientos y controles de seguridad de la información de acuerdo con su clasificación, sistemas, reevaluación de riesgos y procesos del negocio involucrados en la prestación de servicios con terceros.

Es deber del tercero implementar cambios que no degraden la seguridad de la información en ningún momento, contando con los requerimientos de este desde su diseño hasta su implementación.

5.12. Gestión de incidentes en la seguridad de la información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se gestionarán los incidentes de seguridad de la información en todos sus procesos.

5.12.1. Responsabilidades y Procedimientos

En EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se definirá y establecerán responsabilidades y el procedimiento de gestión de incidentes, eventos y vulnerabilidades de seguridad de la información debido a asegurar una respuesta rápida, eficaz y ordenada de estos.

Todos los CEAS involucrados de forma total o parcial en un incidente, o que tengan conocimiento de un evento o vulnerabilidad de seguridad de la información, deberán reportar al CONSORCIO a través del correo electrónico mesadeservicios@seguridadcea.com de forma inmediata y oportuna sobre el mismo con la finalidad de darle cierre al mismo.

5.12.2. Reporte de Eventos de Seguridad de la Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS todos los eventos de seguridad de la información deben ser informados o reportados oportunamente por los CEAS y funcionarios a través de los canales de gestión establecidos por la empresa.

5.12.3. Reporte de Vulnerabilidades de Seguridad de la Información

En EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, todos los CEAS y colaboradores que hacen uso de cualquier activo de información o utilizan servicios o sistemas de información de la empresa. deben reportar cualquier hallazgo, debilidad o vulnerabilidad, o sospecha que pueda poner en riesgo la seguridad de la información. Así mismo, el equipo de desarrollo de la Plataforma Tecnológica AULAPP deberá realizar todas las revisiones pertinentes para detectar y corregir vulnerabilidades de forma temprana.

5.12.4. Evaluación de Eventos de Seguridad de la Información y Decisiones sobre los Mismos

En EL CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, todo evento de seguridad de la información será evaluado y clasificado de acuerdo con la gestión de incidentes establecida.

5.12.5. Respuesta a Incidentes de Seguridad de la Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS todos los incidentes presentados tendrán una respuesta por parte del área o responsable encargado por medio de la herramienta de gestión GLPI o por correo electrónico según sea el caso, así mismo, en el caso que la respuesta sea para un cliente interno, se dará respuesta con los logs de revisión y con la traza del incidente identificando en cada paso las acciones tomadas.

Los CEAS y funcionarios deberán interactuar de forma dinámica y asertiva en la respuesta al incidente de seguridad de la información, brindando el conocimiento completo de sus procesos con la finalidad de entregar una respuesta que garantice la no repetición de dicho incidente.

5.12.6. Aprendizaje Obtenido de los Incidentes de Seguridad de la Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se mantendrá una base de conocimiento del tratamiento de incidentes ocurridos como parte del aprendizaje para el análisis, respuesta y solución a incidentes posteriores, y a la minimización de impacto de seguridad de la información.

5.12.7. Recolección de Evidencia

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se identificará, adquirirá y preservará la información de las evidencias de los incidentes de seguridad de la información presentados.

En caso de borrado de información, se realizará un proceso de informática forense, ya sea a nivel interno o por medio de algún proveedor que determine la Dirección del CONSORCIO.

Los encargados de realizar el análisis forense deberán disponer de todos los recursos necesarios para que se pueda realizar esta función a cabalidad, sin alterar las evidencias del caso y siguiendo el procedimiento que la Dirección del CONSORCIO establezca.

5.13. Cumplimiento

5.13.1. Cumplimiento de Requisitos Legales y Contractuales

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se cumplirán las obligaciones legales, estatutarias y contractuales relacionadas con la seguridad de la información. Implementando todas las medidas humanas y tecnológicas que garanticen el adecuado cumplimiento de los Requisitos.

Identificación de la Legislación Aplicable y de los demás Requisitos

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se identificarán, documentarán y mantendrán actualizados todos los requisitos legales y otros requisitos relacionados con la seguridad de la información. Estableciendo todas las acciones pertinentes al cumplimiento.

Derechos de Autor y Propiedad Intelectual

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se cumplirán los requisitos contractuales y legales vigentes sobre derechos de autor y propiedad intelectual, uso de software licenciado e información utilizada en la organización para sus operaciones.

Protección de Registros

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se protegerán los registros de todos los procesos contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de acuerdo con los requisitos contractuales, legales vigentes y políticas de seguridad de la información establecidas.

Política de Tratamiento de la información de Datos Personales

De acuerdo con los requisitos legales vigentes relacionados con el tratamiento de la información

de datos personales y al implementar buenas prácticas de seguridad de la información, el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS en calidad de responsable y encargado de los mismos define la Política de Protección de Datos Personales. (Ver documento Política de Protección de Datos de Personales).

Reglamentación de Controles Criptográficos

El CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS establecerá e implementará controles criptográficos de acuerdo con los requisitos contractuales y legales vigentes que preserven la seguridad de la información. Así mismo, se dará prioridad a los cifrados más seguros siempre que la legislación no se actualice para considerar los nuevos algoritmos de cifrado que existan en el mercado.

5.13.2. Revisiones de Seguridad de la información

Revisión Independiente de la Seguridad de la Información

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS permite la revisión periódica cada año y de manera independiente a todos los activos y elementos que hacen parte del CONSORCIO.

Cumplimiento con las Políticas y Normas de Seguridad

La Dirección del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS debe revisar permanentemente el cumplimiento de las políticas de seguridad de la información y tratamiento de datos personales en su área y proceso bajo su responsabilidad de acuerdo con los requisitos contractuales y legales vigentes.

Todos los CEAS y colaboradores del CONSORCIO deberán conocer y dar cumplimiento con las políticas de seguridad y de tratamiento de datos personales según aplique.

Revisión del Cumplimiento Técnico

En el CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS se realizarán revisiones periódicas o cuando se considere necesario sobre el cumplimiento de las reglas y políticas de seguridad en los sistemas de información que hacen parte de las operaciones de su negocio.

Es deber de todos los CEAS y colaboradores del CONSORCIO reportar cualquier módulo de los sistemas de información que manejan que no esté cumpliendo con las políticas de seguridad de la información.

6. PRIVACIDAD Y CONFIDENCIALIDAD

El CONSORCIO y el CEA, se obligarán a guardar bajo reserva y asegurarán que sus representantes, funcionarios, directores, empleados, contratistas, agentes y/o asesores conservarán en confidencialidad toda la información verbal o escrita que sea catalogada como confidencial o que, sin ser catalogada como tal, pueda ser razonablemente considerada como confidencial, recibida de la otra parte. Cada parte considerará los documentos técnicos y comerciales facilitados por la otra como propiedad industrial y/o intelectual de dicha otra parte, y/o de terceros según corresponda, por lo que se respetará su titularidad y las normas de propiedad industrial e intelectual vigentes sobre la materia, lo anteriormente descrito se entiende

como información confidencial.
Las partes se obligan a no hacer uso de las marcas de la otra parte y/o de terceros sin previa autorización o instrucción por parte de sus titulares, en caso del CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS, deberá solicitarse autorización por escrito a través de la Mesa de Ayuda, por medio de ticket al correo electrónico mesadeservicios@seguridadcea.com y por parte del CEA, la autorización la brindará el representante legal, por medio del correo electrónico registrado.
El CONSORCIO y el CEA, se obligan a mantener bajo confidencialidad la existencia del presente documento.

No se considera información confidencial lo siguiente:
I. Sea con posterioridad información disponible para el público en general por otra causa que no sea por incumplimiento de la obligación de confidencialidad conforme al presente documento.
II. Ya fuera conocida por el receptor y el mismo pueda demostrarlo con documentos que ya existían en su poder.
III. Sea revelada al receptor por un tercero sin comprometer obligación alguna de confidencialidad.
IV. Sea preparada por o en nombre de la parte que divulga sin utilizar información confidencial recibida con ocasión del presente documento; o
V. Deba revelarse por disposición de la ley aplicable o de cualquier autoridad gubernamental o judicial.

7. PROPIEDAD INTELECTUAL E INDUSTRIAL

Todos los derechos de propiedad intelectual y/o industrial que el CONSORCIO, ostente o represente sobre productos, software, hardware, licencias, garantías, documentos, información, especificaciones de construcción técnicas y funcionales, aportados por éste en la infraestructura tecnológica y/o sea necesario utilizar para la realización del servicio, serán de propiedad del CONSORCIO, y/o de terceros con los cuales el CONSORCIO cuente con el respectivo licenciamiento.

8. CUMPLIMIENTO

El cumplimiento de la política y los principios de Seguridad de la Información definidas en estas políticas es de carácter obligatorio para todos los actores estipulados en el alcance, el incumplimiento o violación de cualquiera de estas, conlleva a aplicar medidas correctivas y asumir responsabilidades de tipo disciplinario y/o penal a que haya lugar.

9. REVISIÓN

El CONSORCIO es el encargado de efectuar revisiones al texto del presente documento como resultado de su aplicación para adaptarlo a nuevas normas o disposiciones legales sobre la materia que surjan, para la aprobación de este.

10. VIGENCIA

El presente documento entra en vigor a partir de su aprobación por la Dirección del CONSORCIO y deroga todas las directrices o normas y demás disposiciones que le sean contrarias o que se consideren obsoletas.