Política de Seguridad y Privacidad de la Información

CONSORCIO SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA CEAS Y CIAS

DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

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.

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.

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.

1. 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.

1.1 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

- 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 los mismos y por ende del Sistema de Control y Vigilancia Aulapp.

2. 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.

2.1 CONTROL 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.

2.2 ESCRITORIO Y PANTALLA LIMPIA

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.

- Sus funcionarios no almacenen en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles.

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

2.3 EQUIPOS

- 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

2.4 CONECTIVIDAD

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.

3. 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.

3.1 TRATAMIENTO DE LA INFORMACIÓN EN LA OPERACIÓN DEL CEA

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.

3.2 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.

4. POLÍTICA PARA 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 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. REFERENCIAS NORMATIVAS

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.

Resolución 1208 del 05 de mayo de 2017. Por la cual se establecen las condiciones, características de seguridad y los rangos de precios al usuario para servicios prestados por los Centros de Enseñanza Automovilística."