MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CAPTUCOL S.A.S

2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN 2

2. OBJETO 3

3. DEFINICIONES 3

4. AMBITO DE APLICACIÓN 5

5.PRINCIPIOS GENERALES DE ACTUACIÓN……...5

6. POLITICAS DE USO DE RECURSOS INFORMATICOS……6

6. REQUISITO BASICOS DE SEGURIDAD DE LA INFORMACIÓN……...……...9

7.DIRECTRICES DE GESTIÓN Y SUPERVISIÓN……..……10

8. CONTROL Y GESTIÓN DE RIESGOS……10

9. GESTION DE INCIDENTES……..……10

10. SEGUIMIENTO, INTERPRETACIÓN Y REVISIÓN……...……...11

11. DIFUSIÓN DE LA POLITICA…….12

12. MARCO LEGAL - HABEAS DATA ……. ……..12

13. ENTRADA EN VIGOR……..……..12

1. INTRODUCCIÓN:

Con el ánimo de establecer la estrategia de seguridad de la información, CAPTUCOL S.A.S. busca constituir un modelo que permita llevar a cabo nuestro objetivo de seguridad de manejo en la información, buscando niveles de protección y resguardo de la información, definiendo ciertos lineamientos para garantizar el debido control y prevención de los riesgos asociados con la información de la empresa.

CAPTUCOL S.A.S. constituye este modelo de seguridad. Se establece que la administración, control y vigilancia del cumplimiento de esta política está a cargo de la empresa externa CONTROL LEGAL ARANZA ROZO SAS.

2. OBJETIVO:

Por medio del presente documento se pretende divulgar y formalizar una política de seguridad en la información, esto con la finalidad de que cada empleado o persona natural y/o jurídica relacionada con CAPTUCOL S.AS. y que esta vinculada con la información privada y base de datos se acoja y aplique las diferentes estrategias establecidas para proteger los posibles riesgos de daño, perdida y uso indebido de la información, los equipos y demás recursos informáticos de la empresa.

Este documento define los lineamientos que debe seguir CAPTUCOL S.A.S. con relación a la seguridad de la información.

3. DEFINICIONES:

Para los propósitos de este documento se aplican los siguientes términos y definiciones:

- CIBERSEGURIDAD: Actividades tendentes a garantizar, tanto la seguridad de la información, como la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas que puedan verse afectadas por las ciberamenzas.
- DATOS PERSONALES: Toda información sobre una persona física identificada o identificable. Esto incluye cualquier dato que, directa o indirectamente, pueda ser utilizado para identificar a una persona como nombres, fotografías, direcciones de correo electrónico, datos bancarios, información sobre redes sociales, ubicación, o dirección IP de un ordenador, entre otros. Los Datos Personales están protegidos por diversas legislaciones y se deben seguir

prácticas 3 adecuadas para su recogida, tratamiento y almacenamiento de cara a respetar los derechos de privacidad de las personas involucradas

- GESTIÓN DE INCIDENTES: conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un Incidente, resolviéndose e incorporando medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas
- INCIDENTE DE CIBERSEGURIDAD: suceso inesperado o no deseado que pueda comprometer la disponibilidad, autenticidad, trazabilidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por Sistemas de Redes y de Información o accesibles a través de ellos.
- INFORMACIÓN: activo principal de cualquier empresa que puede estar en formato físico, o digital y pueden estar determinados en ficheros de todo tipo (texto, imagen, multimedia, bases de datos…), pasando por los programas y aplicaciones que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.
- CONFIDENCIALIDAD: procura que la información solo sea accesible para los Usuarios autorizados a acceder a ella y que no podrá ser divulgada a terceros sin la correspondiente autorización.
- PRINCIPIO DE INTEGRIDAD: pretende asegurar que los datos se mantendrán libres de modificaciones no autorizadas y que la información existente no ha sido alterada por personas o procesos no autorizados.
- RIESGO: la posible pérdida o perturbación causada por un Incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal Incidente.
- TRATAMIENTO DE DATOS: Cualquier operación o conjunto de operaciones realizadas sobre Datos Personales, o conjuntos de éstos, ya sea por procesos automatizados o no, como la recogida, 5 registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- VULNERABILIDAD: Cualquier debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado.
- CONTRASEÑA: Clave de acceso a un recurso informático.
- DIRECTRICES: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
- PROTECTOR DE PANTALLA: Programa que se activa a voluntad del usuario ó automáticamente después de un tiempo en el que no ha habido actividad.
- RECURSOS INFORMATICOS: Elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores

portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y dato

- SESIÓN: Conexión establecida por un usuario con un Sistema de Información.
- USUARIO: Toda persona que pueda tener acceso a un recurso informático de captura de vehículos CAPTUCOL.
- USUARIO DE RED: Usuarios a los cuales CAPTUCOL les entrega un identificador de cliente para acceso a sus recursos informática.
- USUARIOS EXTERNOS: Son aquellos clientes externos que utilizan los recursos informáticos de CAPTUCOL a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.

4. AMBITO DE APLICACIÓN:

La presente política es aplicable a todos los empleados de CAPTUCOL S.A.S, así como a sus proveedores y clientes que presten servicios o se relaciones directamente con la empresa.

5. PRINCIPIOS GENERALES DE ACTUACIÓN:

CAPTUCOL S.A.S. es consciente de que la seguridad de la información es un elemento fundamental para proteger los activos e información de la empresa, esto basado en la efectiva gestión y control de riesgos, con el fin de lograr cumplir sus objetivos, en ese sentido, se compromete a divulgar y aplicar con todas las áreas de la empresa el buen funcionamiento de los medios informáticos, a través de estrategias que contribuyen a una buena gestión de la seguridad en estos sistemas de información.

De conformidad con lo anterior, todos los empleados de CAPTUCOL S.A. deberán respetar y guiar su actuación con base en los siguientes principios:

I. **Proceso integral basado en la gestión y control de riesgos:** CAPTUCOL S.A.S. lleva a cabo una gestión de la seguridad de la información que se fundamenta en los principios de gestión y control de riesgos, la cual pretende identificar y evaluar los riesgos con el fin de llevar un control sobre los mismos.

II. **Definición, desarrollo y mantenimiento:** para lograr la puesta en marcha de los objetivos, estrategias y compromisos asumidos, CAPTUCOL S.A.S. impulsará el desarrollo de un Sistema de Gestión integrado por los controles técnicos, legales y de gestión de la seguridad de la información necesarios para garantizar en todo momento el cumplimiento de los

requisitos legales, reglamentarios y contractuales en la materia que le sean de aplicación, CAPTUCOL aplicara y aprobara las políticas y/o procedimientos específicos por materia que desarrollarán los principios y requisitos básicos de seguridad de la información establecidos en la presente Política

III. **Promoción de una cultura de seguridad de la información:** CAPTUCOL S.A.S. se compromete a promover de forma activa una cultura de seguridad de la información entre todos sus empleados, ya sea internamente, o entre sus clientes y proveedores. I

IV. **Protección proactiva:** CAPTUCOL S.A.S. elabora la presente política de manera que se persiga proactivamente la salvaguarda de los niveles establecidos de confidencialidad, disponibilidad, autenticidad, trazabilidad e integridad parar sus activos de información.

V. **Mejora continua:** La empresa pretende lograr un progreso ininterrumpido de todos los procesos vinculados a la protección de la seguridad de la información de las redes y de los Sistemas de Información, de tal forma que contribuya a que todo CAPTUCOL S.A.S. sea digitalmente resiliente.

6. POLITICAS DE USO DE RECURSOS INFORMATICOS:

- El uso de cualquier sistema de información y demás recursos informáticos por parte del empleado, trabajadores o usuarios de los sistemas de la CAPTUCOL S.A.S. debe someterse a todas las instrucciones técnicas, que imparta la entidad.
- Los recursos informáticos de CAPTUCOL S.A.S. dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la empresa y estará catalogado como lo consagran las políticas de la Entidad. Cualquier otro uso está sujeto a previa autorización del gerente.
- Para el uso de los recursos tecnológicos de CAPTUCOL S.A.S. todo usuario debe firmar un acuerdo de confidencialidad y antes de que le sea otorgado su acceso a la red y sus respectivos privilegios o medios de instalación.
- La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada con autorización de captura de vehículos CAPTUCOL S.A.S.
- Todo usuario o empleado es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios o empleados no deben permitir que ninguna otra persona realice labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo

hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de CAPTUCOL S.A.S.

- Un usuario o empleado puede ser monitoreado bajo previa autorización del gerente y directivos de la empresa.
- Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encriptación y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.
- Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.
- A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al gerente de la empresa.
- Si el usuario o empleado está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.
- Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico admin@captucol.com.co.
- Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no sean utilizados.
- Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad corto la aplicación deberá cerrar la sesión iniciada por el usuario.
- La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.
- Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (correo, ingreso a plataforma) y a los administradores de los mismos.
- Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores.
- Todos los usuarios deben ser automáticamente forzados a cambiar su contraseña por lo menos una vez cada 30 días.
- Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales.

- Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras y caracteres especiales.
- No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es "Enero-2004" que según la política "Contraseñas fuertes", es una contraseña válida, pero al mes siguiente pasa a ser "Febrero-2004" y así sucesivamente.
- El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente.
- Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.
- Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean empelados de la empresa, ningún usuario deberá intentar obtener contraseñas de otros usuarios.
- Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 min. Por otra parte, el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.
- Si se transporta información sensible en medios legibles por el computador (disquetes, cintas magnéticas, CD´s, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.
- Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.
- Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción, lo anterior con autorización del gerente.
- Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto, podrá ser supervisada por el superior inmediato del empleado.
- Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.
- La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.
- Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

- Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros ó que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.
- En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y eliminarlo.
- La publicación de logos, marcas o cualquier tipo de información sobre captura de vehículos CAPTUCOL S.A.S. solo podrá ser realizada a través de las páginas autorizadas de la misma y previa autorización de la gerencia. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.
- Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación.

7. REQUISITOS BASICOS DE LA SEGURIDAD DE INFORMACIÓN:

Para llevar a cabo la gestión diaria de la seguridad y un eficaz funcionamiento y aplicación la información, se procederá siempre conforme a los siguientes requisitos básicos:

• Establecer requerimientos de seguridad desde el diseño y por defecto.

• Prevención, detección, respuesta y conservación.

• Vigilancia continuada y reevaluación periódica.

• Diferenciación de responsabilidades.

• Organización e implantación del proceso de seguridad.

• Análisis y gestión de los Riesgos.

• Gestión del personal.

• Autorización y control de los accesos.

• Protección de las instalaciones.

• Adquisición de productos de seguridad y contratación de servicios de seguridad.

• Mínimo privilegio.

• Integridad y actualización del Sistema de Información.

• Protección de la Información almacenada y en tránsito.

• Prevención ante otros sistemas de Información interconectados.

• Registro de la actividad y detección de código dañino.

• Incidentes de seguridad.

• Continuidad de la actividad.

• Mejora continua del proceso de seguridad.

• Seguridad en la cadena de suministro.

• Confiabilidad, seguridad y resiliencia.

Cada uno de estos requisitos se desarrollará por los correspondientes procedimientos y/o políticas específicas aprobadas internamente.

- Se establece la figura de Superadministradores, quienes tienen la facultad única de asignar o controlar los accesos. Los usuarios finales tienen un acceso limitado y segmentado estrictamente a la información necesaria para su labor (Principio de Mínimo Privilegio).
- Parámetros de Contraseñas: Deben contener mínimo 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales (@, #, $, etc.).
- Restricción de Doble Acceso: Los sistemas cuentan con validación de IP y Código de Seguridad. Se prohíbe el ingreso simultáneo de una misma cuenta desde dos ubicaciones o dispositivos diferentes.
- Bloqueo y Eliminación por Inactividad:
    - Todo acceso a plataforma se bloqueará automáticamente tras 3 minutos de inactividad.
    - Caso Investigadores: Las cuentas de los investigadores serán auditadas mensualmente. Si se detecta falta de uso o incumplimiento de las metas establecidas, el acceso será eliminado definitivamente.
- Seguridad de Dominios y Respaldos: La empresa cuenta con dominios web protegidos mediante certificados de seguridad (SSL - icono de candado). Se realizan respaldos periódicos de toda la información crítica para garantizar la disponibilidad ante desastres.

8. DIRECTRICES DE GESTIÓN Y SUPERVISIÓN:

Corresponde a captura de vehículos CAPTUCOL a través de la presente Política establecer las estrategias y directrices de gestión en materia de seguridad de la Información. A su vez, es competencia del área de **CONTROL LEGAL ARANZA ROZO S.A.S.** velar por la implementación y desarrollo de la presente Política y de las medidas adoptadas en aplicación de la misma, así como revisar, y en su caso, proponer a los empleados de la empresa la presente Política.

9. CONTROL Y GESTIÓN DE RIESGOS:

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los Riesgos a los que están expuestos. Ante cualquier evento que comprometa la seguridad (pérdida de datos, sospecha de hackeo, etc.), el empleado tiene la obligación de comunicarse de inmediato con CONTROL LEGAL ARANZA ROZO SAS a través del canal oficial: GESTIÓN DE INCIDENTES:

Las áreas que conforman CAPTUCOL S.A.S deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por Incidentes de ciberseguridad. Para ello, de conformidad a lo recogido en el procedimiento correspondiente, dichas áreas deben implementar las medidas mínimas de seguridad determinadas por la normativa aplicable, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos0.

CAPTUCOL S.A.S. mantiene sus plataformas y bases de datos alojadas en una infraestructura de Servidores Privados Virtuales (VPS) de alta disponibilidad a través del proveedor DigitalOcean. Esta infraestructura cuenta con recursos dedicados que garantizan un rendimiento óptimo y una capa de seguridad perimetral activa mediante un Firewall de red por defecto, el cual es administrado y monitoreado por CONTROL LEGAL ARANZA ROZO SAS.

Los usuarios reconocen que la seguridad del entorno está protegida por estas barreras de hardware y red, y que cualquier modificación o intento de vulnerar estas protecciones será reportado como un incidente grave.

10. SEGUIMIENTO, INTERPRETACIÓN Y REVISIÓN:

10.1. Seguimiento: El cumplimiento de esta Política será supervisado por CONTROL LEGAL ARANZA ROZO SAS, Se establecerán mecanismos de auditoría y revisión periódica para asegurar que la empresa cumpla con los estándares establecidos. En caso de tener algún

problema, o detectar un Incidente que pueda afectar al funcionamiento o seguridad de los Sistemas de Redes y sistemas, y/o la seguridad de las mismas, este se deberá comunicar inmediatamente a su jefe inmediato a través de los canales habilitados.

10.2. Interpretación: El órgano de contacto para cualquier duda y/o consulta en relación con la interpretación y ejecución de la presente Política será CONTROL LEGAL ARANZA ROZO SAS.

10.3. Revisión y Actualización: Esta Política será revisada y, en su caso, actualizada periódicamente para adaptarse a las necesidades y/o cambios regulatorios, organizativos y técnicos, así como para incorporar las mejores prácticas identificadas en la empresa. La modificación y/o actualización de la presente Política será aprobada por Martha Helena Morales Guacaneme, representante legal de CAPTUCOL S.A.S.

11. DIFUSIÓN DE LA POLITICA:

Esta Política será publicada en nuestra página web ww.captucol.com, adicionalmente se llevará a cabo periódicamente acciones de comunicación, formación y sensibilización para la comprensión y puesta en práctica de esta Política a través de diferentes canales, así como de sus actualizaciones. En todo caso, es responsabilidad de todos los empleados y proveedores leer y comprender el contenido de esta Política, así como observar y cumplir sus directrices, principios y procesos en el desarrollo de su trabajo, en la medida en que el desconocimiento de todo o parte de su contenido no exime de su cumplimiento. En este sentido, se recomienda acceder de forma periódica al contenido de esta Política a través de los canales disponibles para una mejor comprensión de la misma.

12. MARCO LEGAL (HABEAS DATA)

En cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013, CAPTUCOL S.A.S. garantiza la protección de datos personales. Cuando se traten datos personales no públicos, se aplicarán los principios de libertad, veracidad, transparencia y seguridad. Cualquier titular podrá ejercer su derecho de Habeas Data contactando al oficial de privacidad delegado.

13. ENTRADA EN VIGOR:

La presente Política fue aprobada por Martha helena Morales Guacaneme representante legal de CAPTUCOL S.A.S. el día 01 de enero de 2026, entrando en vigor desde el momento de su publicación y/o divulgación.