POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CAMACOL
CÁMARA COLOMBIANA DE LA CONSTRUCCIÓN

CÁMARA COLOMBIANA DE LA CONSTRUCCIÓN CAMACOL

1. Objetivo:

Establecer las directrices, lineamientos, responsabilidades y conductas que seguirán todos los colaboradores de Camacol para mantener los principios de confidencialidad, integridad, disponibilidad y privacidad de la información, desarrollando habilidades y conocimientos requeridos para tener y aplicar buenas prácticas de Seguridad de la Información y Ciberseguridad, de acuerdo con las necesidades de la compañía y las normativas que apliquen.

2. Alcance:

Esta Política aplica a todas las partes interesadas (Altos Directivos, Empleados, clientes, proveedores y/o contratistas de la Compañía, entre otros, estos deberán manifestar su conocimiento y aceptación respecto de su obligación de cumplir con las normas relacionadas con la seguridad de la información.

3. Seguridad De La Información:

Seguridad de la Información, es el conjunto de medidas que tienen como fin proteger y mantener los principios de confidencialidad, integridad y disponibilidad de los Activos de Información de Camacol, con el fin de prevenir incidentes tanto accidentales como intencionados, mediante la implementación de controles y medidas asociadas con las personas, los procesos y la tecnología, a la luz de las mejores prácticas y la alineación con los objetivos estratégicos de Camacol, gestionando estrictamente el cumplimiento de obligaciones legales y regulatorias, fortaleciendo así la imagen y posición del gremio.

La Seguridad de la Información se caracteriza por la preservación de:

a. Su **Confidencialidad**, asegurando que sólo quienes estén autorizados puedan acceder a la Información.
b. Su **Integridad**, asegurando que la Información y sus métodos de proceso sean exactos y completos.
c. Su **Disponibilidad**, asegurando que los usuarios autorizados tengan acceso a la Información cuando lo requieran.

4. Principios De Seguridad De La Información

Con el fin de dar cumplimiento al marco normativo, regulatorio y a los objetivos de negocio, Camacol ha definido los siguientes principios fundamentales como soporte a la Política:

a. La Información es uno de los activos más importantes de CAMACOL, y por tanto será utilizada acorde con los procesos del negocio, sus condiciones y regulaciones.
b. La confidencialidad de la Información será mantenida, sin importar su medio, forma, sea física o digital o su estado, almacenada o en tránsito.
c. La Información preservará su integridad independientemente de su ubicación, forma de almacenamiento y del canal de comunicación por el que sea transmitida.
d. La Información estará disponible cuando sea requerida, en el formato y tiempo necesarios para una ejecución exitosa de las operaciones.
e. CAMACOL velará por el cumplimiento de las regulaciones legales vigentes en materia de Seguridad de la Información que le apliquen.
f. La privacidad de la Información de CAMACOL, de sus clientes, afiliados, contratistas, proveedores, colaboradores y usuarios será preservada.
g. Se mantendrá la trazabilidad de las acciones realizadas sobre la Información de CAMACOL durante el ciclo de vida de esta.

5. Ciberseguridad

Ciberseguridad, es el conjunto de políticas, conceptos de seguridad, recursos, controles de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación, desarrollo, formación y buenas prácticas en general, utilizadas para prevenir y proteger los datos, sistemas y aplicaciones, preservando los principios de la Seguridad de la Información e incluyendo las características de:

a. Control de accesos: Proceso mediante el cual se permite o no el acceso de un usuario a aplicaciones, servidores, equipos tecnológicos entre otros, según los perfiles asignados.
b. No repudio: Condición por medio de la cual no se puede negar la ejecución de una actividad realizada sobre la plataforma tecnológica, de acuerdo con los registros de auditoría o log's.

6. Principios De La Ciberseguridad

Con el fin de dar cumplimiento al marco normativo, regulatorio y a los objetivos de CAMACOL, se consideran los siguientes principios de la Ciberseguridad para preservar la información y correcto funcionamiento de la plataforma tecnológica para que no se afecten los procesos de la Entidad:

a. **Mínimo privilegio**: Son todos aquellos privilegios que tienen los sistemas y aplicaciones que se encuentran interconectados pero que solo deben tener los usuarios, configuración y conexión de red necesarios para que funcionen de acuerdo con lo requerido por el proceso.

b. **Mínima superficie de exposición**: Deben diseñarse las tareas o actividades a realizar en cada uno de los procesos de CAMACOL, de tal forma que no queden o se habiliten canales, privilegios, IP's, usuarios, publicación o puertos que faciliten a un ciberdelincuente acceder a los sistemas, producto de estas debilidades de configuración en la red y plataforma tecnológica.

c. **Defensa en profundidad**: Debe existir seguridad por niveles o anillos, es decir, que la arquitectura de red o controles de ciberseguridad que se implementen, tales como: firewall, IPS, IDS, Antivirus, WAF, antispam, honeypot, etc., deben configurarse en diferentes zonas de red. Así como usar diferentes dispositivos para dificultar el trabajo de un ciberdelincuente, obstaculizando su paso por las diferentes capas y evitando que cumpla con su objetivo.

7. Objetivos De Seguridad De La Información

Los siguientes son los objetivos en materia de Seguridad de la Información y Ciberseguridad definidos por CAMACOL:

a. Cumplir con las obligaciones legales vigentes relacionadas con Seguridad de la Información y Ciberseguridad que apliquen a la Entidad, tomando las medidas necesarias de acuerdo con la operación que se realiza en CAMACOL.
b. Gestionar los riesgos de Seguridad de la Información y Ciberseguridad en todos los procesos de manera eficiente, con el fin de proporcionar continuidad y calidad a las operaciones de CAMACOL.
c. Facilitar la discusión al interior de la Entidad en temas de Seguridad de la Información y Ciberseguridad, ayudando a que todos los colaboradores, clientes y contratistas sean conscientes de las amenazas potenciales de Seguridad de la Información y Ciberseguridad con los riesgos asociados a la entidad.
d. Soportar y mejorar la calidad de las operaciones de CAMACOL, permitiendo un equilibrio entre funcionalidad y seguridad, a la luz de las mejores prácticas de la industria.

8. Política General De Seguridad De La Información Y Ciberseguridad

Para CAMACOL, la información es considerada como uno de los activos importantes para el negocio y los procesos que soportan su operación, por este motivo se implementan buenas prácticas de Seguridad de la Información y Ciberseguridad que permiten cumplir con la normativa o requerimientos legales aplicables de los Entes de Control.

CAMACOL encamina los esfuerzos de los colaboradores y recurso técnico, para preservar la información y conservar la confidencialidad, integridad y disponibilidad de los activos de información, protegiendo y asegurando en el ciberespacio, los datos, sistemas y aplicaciones que son esenciales para la operación de la Entidad. Igualmente, CAMACOL se compromete a proteger los datos sensibles, ejecutando los procesos de manera óptima y manteniendo su privacidad.

Por tanto, CAMACOL debe:

a. Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad.
b. Establecer que todos los colaboradores y terceros son responsables de registrar y reportar las violaciones y eventos sospechosos de Seguridad de la Información y Ciberseguridad, de acuerdo con los procedimientos correspondientes.
c. Clasificar, proteger y asignar responsables de los Activos de Información, de acuerdo con la metodología que se establezca y con los criterios de valoración, en relación con la importancia que posee para la Entidad. Realizando igualmente el análisis de riesgos correspondiente, para definir los controles que preserven la información y plataforma tecnológica de la Entidad.
d. Establecer los requisitos y buenas prácticas de Seguridad de la Información y Ciberseguridad, uso aceptable y controles relacionados con el acceso y utilización de los activos de la información de CAMACOL, que mantengan y protejan las características de confidencialidad, integridad y disponibilidad de éstos.
e. Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad de forma oportuna.
f. Administrar los programas de Ciberseguridad de la entidad, esto lo realizara el proveedor externo de tecnología, ellos deberán generar alertas en caso de que detecten que se está vulnerando la seguridad de la información o la organización está sufriendo un ataque cibernético.
g. Discutir los casos que violen la presente política en el comité de tecnología y aplicar los planes de acción y sanciones que sean necesarios.

9. Cumplimiento De La Política

El cumplimiento de la Política de Seguridad de la Información y Ciberseguridad es obligatorio. Cada colaborador de Camacol, colaborador temporal, pasante, tercero, personal interno, personal externo y contratista que tenga algún vínculo con los procesos o que acceda a la información, entenderá su rol y asumirá su responsabilidad respecto a los riesgos en Seguridad de la Información y Ciberseguridad, de acuerdo con las políticas definidas.

El incumplimiento de esta Política General podrá acarrear sanciones, de acuerdo con los procedimientos establecidos para tal fin en la organización.

10. Historial de cambios

Versión	Descripción	Fecha emisión
0	Creación del documento	01/11/2020