Política de seguridad de la información

GENERALIDADES:

Certicámara está comprometida en proteger y cuidar la información de sus clientes, colaboradores, proveedores y aliados, es por esta razón que reconoce que la información es un activo fundamental en la prestación de sus servicios y en la toma de sus decisiones.

Para dar cumplimiento se han adoptado mejores prácticas y se ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI), el cual está conformado por políticas, estándares técnicos y generales de seguridad de la información, procesos y procedimientos, estructura organizacional y mecanismos de verificación y control; tiene como propósito garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, asumidos, gestionados y mitigados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Las Políticas de Seguridad de la Información y Ciberseguridad son elementos fundamentales dentro del SGSI puesto que contienen directrices que enmarcan la actuación de todos los empleados, proveedores y visitantes de Certicámara.

OBJETIVO:

Proteger, preservar y administrar objetivamente la información de **Certicámara** junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los atributos de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Política de seguridad de la información

PRINCIPIOS:

Los principios de seguridad para el manejo de la información y que corresponden a los exigidos por la Ley, que tendrá en cuenta **Certicámara** son:

- Confidencialidad: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- Integridad: propiedad de exactitud y completitud.
- Disponibilidad y no repudio: propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

MARCO LEGAL Y/O TÉCNICO

- NTC – ISO – IEC 27001:2013 Sistema de gestión de seguridad de la información.
- CEA-4.1-10 Criterios específicos de acreditación. Entidades de certificación digital.
- Trust Service Principles and Criteria for Certificaction Authorities 2.0.

Política de seguridad de la información

REQUISISTOS DE SEGURIDAD DE LA INFORMACIÓN:

Certicámara cumple con los siguientes requisitos de seguridad de la información, con el fin de mitigar los posibles riesgos que puedan afectar la organización:

- Se identifica, clasifica y define los propietarios de los activos de información de acuerdo con su sensibilidad y criticidad que soportan los procesos.
- Se identifica y analiza las amenazas y vulnerabilidades de los activos y evallua la probabilidad de ocurrencia e impacto de acuerdo con los principios de seguridad, para determinar el nivel de riesgo existente.
- Se identifica, analiza y trata los riesgo (mitigar, transferir, aceptar, evitar), con el fin de llevar el riesgo a un nivel aceptable.
- Implementa actividades de monitoreo que permiten medir la eficacia de los controles implementados para generar oportunidades de mejora.
- Se realiza seguimiento a los requisitos legales, estatutarios, de reglamentación, normativo y contractuales que tanto **Certicámara** como el cliente y proveedores deben cumplir y que puedan afectar la seguridad de la información.
- Determina los requisitos para el manejo, procesamiento, almacenamiento, comunicación y archivo de la información de cada uno de los servicios de certificación digital.
- Cuenta con los logs de eventos y auditorías, con el fin de determinar lo sucedido en un momento determinado.

Política de seguridad de la información

ESTRATEGIAS

- **Certicámara** implementa programas de formación, sensibilización y toma de conciencia en materia de seguridad de la información.
- El Comité de Presidencia asegura que las políticas de la organización se traduzcan en reglas de conducta y procedimientos que orienten la actuación de la empresa. De igual manera, hará seguimiento al cumplimiento de las actividades de planeación, implementación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

RESPONSABLES:

El Gerente de Gobierno, Riesgo y Cumplimento junto con el Coordinador de Seguridad y Protección de Datos Personales son los responsables de:

- Liderar la implementación de los controles exigidos por la Ley y la normatividad vigente.
- Velar por las respectivas actualizaciones de esta Política, y los ajustes solicitados por los dueños de procesos a la documentación publicada en el sistema de gestión, alineándola al estándar internacional ISO 27001 y sus normas derivadas.

Política de seguridad de la información

El Comité de seguridad de la información recomendará los cambios a la Política, los procesos, los procedimientos, lineamientos y formatos específicos, alineados al estándar internacional ISO 27001 y sus normas derivadas.

Todos los colaboradores de **Certicámara** serán responsables del manejo de la información, el cumplimiento de las políticas y de los controles implementados por la organización, así como de reportar los incidentes de seguridad e implementar acciones correctivas o preventivas a que haya lugar según sus competencias, para asegurar un proceso permanente de mejora en la Gestión de la Seguridad de la Información.

o.

Política de seguridad de la información

Política para la Gestión de Vulnerabilidades

Toda infraestructura tecnológica nueva o modificada (sistemas de información, aplicaciones, servicios de comunicación, etc.) está expuesta a múltiples amenazas, razón por la cual es necesario realizar un análisis de vulnerabilidades técnicas con el fin de evitar incidentes perjudiciales que puedan comprometer la continuidad de la prestación de los servicios a nuestros clientes.

Para llevar a cabo dicho análisis, la Gerencia TIC deberá entregar a la Gerencia de Gobierno, Riesgo y Cumplimiento, el inventario de la infraestructura tecnológica que será objeto de la gestión de vulnerabilidades para definir y delimitar el alcance de dicha gestión. De igual forma, la Gerencia de Gobierno, Riesgo y Cumplimiento será la responsable de la gestión de vulnerabilidades y debe asegurar que se realice como mínimo una vez al año un test y re-test.

Las vulnerabilidades detectadas serán clasificadas, de acuerdo con lo establecido por el common vulnerability scoring system (CVSS) con la finalidad de priorizar los planes de tratamiento de dichas vulnerabilidades.

La Gerencia de Gobierno, Riesgo y Cumplimiento deberá presupuestar y asignar los respectivos recursos para el cumplimiento a las disposiciones de esta política.