# POLÍTICAS DE SEGURIDAD

V1.0

# Contenido

**Control de Versiones**

| Versión | Modificado por | Fecha | Aprobado por |
|---|---|---|---|
| 1.0 | Steven Chiriboga | 10/04/2023 | Mónica Maldonado |

# 1. OBJETIVO

Especificar las condiciones y procedimientos relativos a la seguridad de la infraestructura de la Entidad de Certificación de Información y seguridad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica de Alpha Technologies CIA. LTDA.

# 2. MARCO NORMATIVO

- Ley de Comercio Electrónico, Firmas y Mensajes de Datos, vigente.
- Reglamento a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos vigente.
- Resolución ARCOTEL-CTHB-CTDS-2022-0225

# 3. DECLARACIÓN DE POLÍTICAS DE SEGURIDAD

## 3.1. Procedimientos de seguridad para el manejo de posibles eventos

### 3.1.1. Seguridad de la clave privada de la Entidad de Certificación de Información y Servicios Relacionados Acreditada se vea comprometida

Alpha Technologies posee procedimientos para la seguridad de la clave privada que posee como Entidad Certificadora cumpliendo con controles físicos, lógicos y con políticas de seguridad descritos a continuación:

**Controles físicos:**

Se implementan protecciones físicas y lógicas para evitar la emisión de certificados no autorizados. La protección de la clave privada de la Entidad Certificadora fuera del sistema cifra su clave privada con un algoritmo y una longitud de clave que es capaz de resistir ataques criptoanalíticos durante la vida residual de la clave cifrada o parte de la clave.

Se garantiza que todos los sistemas que firman Certificados y CRL o generan respuestas OCSP utilizan FIPS 140-2 nivel 3 como el nivel mínimo de protección criptográfica.

**Controles lógicos:**

- Conexión con cifrado fuerte entre el personal autorizado y los servidores.
- Acceso a través de un único servidor.
- Permisos de conexión para una IP específica.
- Esquema de seguridad perimetral.

**Políticas de seguridad**

- Acceso restringido sólo autorizado al personal correspondiente.
- Todo acceso será registrado tanto por el técnico asignado como por el sistema a través de logs del sistema.
- Para accesos con permisos de root es necesario la aprobación del gerente técnico.
- Las claves tendrán un tamaño mínimo de 16 caracteres y serán actualizadas cada mes.

## 3.1.2. Sistema de seguridad de la Entidad de Certificación de Información y Servicios Relacionados Acreditada ha sido vulnerado

Cuando el sistema de seguridad ha sido vulnerado, se considera como un incidente de seguridad, el cuál será gestionado por el equipo técnico de la entidad certificadora y el centro de operaciones de seguridad, el procedimiento a seguir si se presenta una vulnerabilidad es:

- Reportar el incidente a la mesa de soporte.
- Asignar el caso al técnico de seguridad informática.
- El técnico se encarga de validar, investigar y realizar actividades para la resolución del incidente mostrado.
- Implementar una solución para disminuir el riesgo que el incidente se vuelva a presentar.
- Se realiza un informe de los hallazgos y actividades realizadas para solucionar el incidente.

### 3.1.3. Si se presentan fallas en el sistema de la Entidad de Certificación de Información y Servicios Relacionados Acreditada que comprometan la seguridad, disponibilidad y prestación de los servicios

La infraestructura posee un diseño de alta disponibilidad, el cual garantiza la disponibilidad del sistema, teniendo respaldos de las aplicaciones del sistema y de las bases de datos para que la información esté disponible en caso de fallas. Existe alta disponibilidad en los servicios de Internet para las conexiones con la infraestructura.

## 3.2. Plan de contingencia para garantizar la continuidad y disponibilidad de los servicios de certificación de información y servicios relacionados con la firma electrónica

Alpha Technologies posee un plan de contingencia considerando factores internos y externos para garantizar la continuidad y disponibilidad de los servicios ante un evento alterador a la continuidad de negocio. Al ejecutar los diferentes procedimientos descritos en el plan de contingencia, se realizará un informe indicando todas las actividades realizadas.

## 3.3. Procedimientos y mecanismos de seguridad para resguardo y conservación segura de la información relativa a la emisión de certificados e información proporcionada por los usuarios.

La información recolectada para la emisión de los certificados digitales posee los siguientes mecanismos y procedimientos:

- La información será almacenada en el sistema con acceso solo al personal autorizado.
- La información solo estará disponible para las aplicaciones autorizadas.

El usuario conoce los datos que son entregados y serán evaluados para el procedimiento de validación.
Los certificados de firma electrónica cumplen los siguientes mecanismos:

- Solo se almacenará el certificado de firma electrónica pero no su clave privada.
- Estarán disponibles las listas CRL y OSCP a todo público.
- Se encontrarán los certificados raíz e intermedio a través de URLs de descarga.