TRIBUNAL CONTENCIOSO
ELECTORAL DEL ECUADOR

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

25 de noviembre 2024
PO-2024-01
V 1.0

Contenido

1. Antecedentes

El presente documento de Política de Seguridad de la Información, establece el marco de referencia a través del cual el Tribunal Contencioso Electoral implementa el Sistema de Gestión de Seguridad de la Información (SGSI) institucional, fijando así los estándares de seguridad de la información a aplicar para proteger adecuadamente sus activos de información.

De conformidad a lo establecido en el Acuerdo Ministerial No. 2024-003 del Ministerio de Telecomunicaciones y de la Sociedad de la Información, emitido el 8 de febrero de 2024 y publicado en Registro Oficial Tercer Suplemento No. 509 de fecha 1 de marzo de 2024, mediante el cual se emite el Esquema Gubernamental de Seguridad de la Información – EGSI v3.0, y conforme la normas NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27005; El Tribunal Contencioso Electoral considera los siguientes elementos centrales para guiar las actividades relacionadas con la seguridad de la información:

1. El compromiso de la máxima autoridad con la seguridad de la información y su mejora continua en todo el Tribunal Contencioso Electoral.
2. La concientización del personal de la importancia de realizar una buena gestión con los activos de información y de los beneficios que se logra con la implementación de un Sistema de Gestión de Seguridad de la Información.
3. El precautelar la disponibilidad, integridad y confidencialidad de la información.
4. La implementación, mantención, monitoreo y mejoramiento continuo de la aplicación de la presente política.
5. El levantamiento y categorización de los activos de información, y sus responsables.
6. La gestión de riesgos que afecten a los activos de información, frente a amenazas y vulnerabilidades.
7. La implementación, supervisión, revisión y mejora continua de los controles de seguridad de la información.
8. La operación correcta y segura de las instalaciones de procesamiento de información.
9. La seguridad física y del entorno donde se encuentran y operan los activos de información.
10. La relación con usuarios y terceras partes vinculadas al Tribunal Contencioso Electoral.

2. Objetivo de la Política

Establecer las políticas y lineamientos que permitan garantizar la adecuada protección de la confidencialidad, integridad y disponibilidad de los activos de información, y que faciliten la preparación de una adecuada gestión de riesgos.

3. Política de Seguridad de la Información

3.1. Descripción de la Política

La máxima autoridad y el personal del Tribunal Contencioso Electoral, considerando la importancia de una adecuada gestión de la información y observancia de las leyes y normativas vigentes, se comprometen a la implementación del Sistema de Gestión de Seguridad de la Información, en concordancia con los principios de confidencialidad, integridad y disponibilidad de los activos de información, promoviendo una gestión eficaz de riesgos y generando una cultura de seguridad de la información que brinde un marco de confianza a los usuarios de los servicios de administración de justicia electoral y en estricto cumplimiento de los objetivos institucionales.

3.2. Declaración de los objetivos de seguridad de la información

Objetivo 1.- Construir una cultura organizacional basada en la seguridad de la información, promoviendo la aplicación y uso de las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, por parte de todo el personal de la institución, usuarios y terceras partes vinculadas, satisfaciendo sus necesidades y expectativas en seguridad de la información.

Objetivo 2.- Gestionar los riesgos en seguridad de la información para mantenerlos en un nivel de aceptabilidad apropiado, que permita minimizar al máximo la probabilidad de violación de seguridad de la información, teniendo como pilar fundamental la implementación de controles de seguridad de la información para el tratamiento de los riesgos.

Objetivo 3.- Defender la confidencialidad, integridad y disponibilidad de la información según sea catalogada como pública, personal, sensible, confidencial, reservada, etc., reduciendo los incidentes de seguridad a un determinado nivel aceptable, de tal manera que se pueda mantener la confianza de los usuarios de los servicios de administración de justicia electoral.

3.3. Roles y Responsabilidades

A continuación se describe los diferentes roles y responsabilidades, con el fin de garantizar en todo momento el adecuado uso y protección de los activos de información del Tribunal Contencioso Electoral:

Máxima Autoridad.- La máxima autoridad a través del Comité de Seguridad de la Información es la responsable de asegurar que la seguridad de la información se gestione adecuadamente en todo el Tribunal Contencioso Electoral.

Comité de Seguridad de la Información (CSI).- Es responsable de gestionar la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información – EGSI v3.0.

Oficial de Seguridad de la Información (OSI).- Es responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información – EGSI v3.0 en el Tribunal Contencioso Electoral.

Jueces, Autoridades Directivas y Responsables de Área.- Son responsables de garantizar que el personal que trabaja bajo su control, protejan la información de acuerdo con las normas establecidas por el Tribunal Contencioso Electoral, para lo cual gestionarán los recursos y brindarán el apoyo requerido.

Custodio de la Información.- Responsable de guardar con cuidado y mantener a buen recaudo el activo de información, estableciendo los mecanismos de protección y precaución que sean necesarios.

Terceras partes vinculadas.- Comprenden los proveedores y otros.

Personal del TCE.- Responsable de cumplir la política de seguridad de la información en la gestión de sus actividades diarias en el Tribunal Contencioso Electoral y tiene la obligación de reportar incidentes de seguridad de la información al OSI.

Propietario del activo.- Aplicable para cualquier tipo de activo de información, el personal propietario tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad del activo, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario de la Información.- En el caso de la información propiamente dicha, el personal propietario es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Propietario del riesgo. – Personal con responsabilidad y autoridad para gestionar un riesgo.

Usuario.- Corresponde a la ciudadanía y/o actores políticos con acceso a los servicios que brinda el Tribunal Contencioso Electoral, ser responsables de dar un buen uso del servicio proporcionado conforme las condiciones establecidas.

3.4. Alcance y usuarios

La presente Política de Seguridad de la Información se apoya y fundamenta en las directrices generales del Esquema Gubernamental de Seguridad de la Información – EGSI v3.0.

Este documento aplica de manera obligatoria a todo el personal del Tribunal Contencioso Electoral y terceras partes vinculadas que tengan acceso a los activos de información de la institución.

Son usuarios de este documento, el personal del Tribunal Contencioso Electoral, terceras partes vinculadas y usuarios de los servicios que brinda el Tribunal Contencioso Electoral.

3.5. Comunicación de la Política

El Tribunal Contencioso Electoral comunicará la Política de Seguridad de la Información a todo el personal y terceras partes vinculadas, mediante la generación de comunicación formal emitida por parte de la máxima autoridad, la realización de eventos de inducción, talleres, capacitaciones, colocación de mensajes lúdicos en sitios estratégicos de la institución, envíos de posts mediante correo electrónico y mensajería, entre otros.

3.6. Excepciones y Exenciones

A la fecha de elaboración de este documento, no se determina excepciones ni exenciones a su cumplimiento.

3.7. Sanciones

En caso de incumplimiento por parte del personal del Tribunal Contencioso Electoral, de alguno de los lineamientos establecidos y de lo descrito en la política, la Unidad de Administración del Talento Humano Institucional, dará inicio al procedimiento de régimen disciplinario conforme a la normativa legal vigente.

3.8. Glosario de Términos

Término	Definición
Activo de información	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la institución.
Amenaza	Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

Análisis de riesgos	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Confidencialidad	Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.
Control de Seguridad	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
CSI	Comité de Seguridad de la Información.
Disponibilidad	Propiedad de la información estar disponible y utilizable en el momento que sea requerido por una entidad autorizada.
EGSI v3.0	Esquema Gubernamental de Seguridad de la Información, versión 3.0.
Evaluación de riesgos	Proceso global de identificación, análisis y estimación de riesgos.
Evento de seguridad de la información	Ocurrencia que indica una posible violación de seguridad de la información o falla de los controles.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
Incidente de seguridad de la información	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
IEC	Comisión Electrotécnica Internacional (International Electrotechnical Commission).
INEN	Servicio Ecuatoriano de Normalización.

Información	Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.
Integridad	Propiedad de proteger la precisión y completitud de los activos.
ISO	Organización Internacional de Normalización (International Organization for Standardization).
Mejora Continua	Metodología para el desarrollo del SGSI, también conocida como ciclo de Deming o círculo PDCA, del inglés Plan-Do-Check-Act.
Norma NTE INEN-ISO/IEC 27001	Seguridad de la Información – Ciberseguridad y Protección de la Privacidad – Sistemas de Gestión de Seguridad de la Información – Requisitos.
Norma NTE INEN-ISO/IEC 27002	Seguridad de la Información, Ciberseguridad y Protección de la Privacidad - Controles De Seguridad De La Información.
Norma NTE INEN-ISO/IEC 27005	Seguridad de la Información — Ciberseguridad y Protección de la Privacidad — Orientación sobre la Gestión del Riesgo de Seguridad de la Información.
NTE	Norma Técnica Ecuatoriana.
OSI	Oficial de Seguridad de la Información.
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Seguridad de la Información	Conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.
SGSI	Sistema de Gestión de Seguridad de la Información.

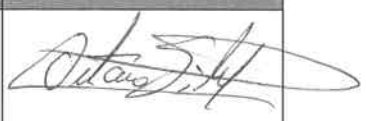
TCE	Tribunal Contencioso Electoral.
Tratamiento de riesgo	Proceso de modificar el riesgo, mediante la implementación de controles.
Violación de la política de seguridad de la información	Comprometimiento de la seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados a la información protegida transmitida, almacenada o procesada de otro modo.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. Documentos de referencia

- Ley Orgánica de Protección de Datos Personales.
- Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024.
- Esquema Gubernamental de Seguridad de la Información - EGSI v3.0.
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27005.
- Plan Estratégico del Tribunal Contencioso Electoral.
- Alcance de la implementación del Esquema Gubernamental de Seguridad de la Información – EGSI v3.0 en el Tribunal Contencioso Electoral.
- Otros.

5. Firmas de responsabilidad

Elaboración:

Nombre del funcionario	Puesto	Unidad	Firma
Ing. José Octavio Silva Peralta	*Oficial de Seguridad de la Información*	*Presidencia*	

Revisión:

Nombre del funcionario	Puesto	Unidad	Firma
Ing. Paulina Santamaría Ramos	*Presidenta del Comité de Seguridad de la Información*	*Planificación*	
Mgs. Francisco Tomalá Medina	*Secretario del Comité de Seguridad de la Información*	*Comunicación*	
Lic. Fernando Mantilla Montenegro	*Miembro del Comité de Seguridad de la Información*	*Talento Humano*	
Dra. Patricia Maldonado Álvarez	*Miembro del Comité de Seguridad de la Información*	*Administrativa Financiera*	
Mgs. William Cargua Freire	*Miembro del Comité de Seguridad de la Información*	*Tecnologías de la Información*	
Dra. María Luisa Paredes Arellano	*Miembro del Comité de Seguridad de la Información*	*Asesoría Jurídica*	
Ab. Álvaro Briceño Córdova	*Miembro del Comité de Seguridad de la Información*	*Delegado de Protección de Datos*	

Control de versiones

Código	PO-2024-01
Versión:	1.0
Fecha de la versión:	25-11-2024
Creado por:	Oficial de Seguridad de la Información del Tribunal Contencioso Electoral
Revisado por:	Comité de Seguridad de la Información del Tribunal Contencioso Electoral
Aprobado por:	Pleno del Tribunal Contencioso Electoral
Nivel de confidencialidad:	Bajo

Historial de cambios

Versión	Fecha	Detalle del cambio
1.0	25/11/2024	Emisión inicial del documento