

REGISTRO OFICIAL

Administración del Sr. Lcdo. Lenín Moreno Garcés
Presidente Constitucional de la República

EDICIÓN ESPECIAL

Año I – N° 84

Quito, miércoles 13 de
septiembre de 2017

LEXIS

CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS
CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN

Art. 107.- Materia no protegible.- No son objeto de protección las disposiciones legales y reglamentarias, los proyectos de ley, las resoluciones judiciales, los actos, decretos, acuerdos, resoluciones, deliberaciones y dictámenes de los organismos públicos, y los demás textos oficiales de orden legislativo, administrativo o judicial, así como sus traducciones oficiales.

Tampoco son objeto de protección los discursos políticos ni las disertaciones pronunciadas en debates judiciales. Sin embargo, el autor gozará del derecho exclusivo de reunir en colección las obras mencionadas en este inciso con sujeción a lo dispuesto en este Capítulo.

Art. 116.- ...

La información y el contenido de las bases de datos producto de las investigaciones financiadas con recursos públicos serán de acceso abierto. Las instituciones o entidades responsables de tales investigaciones deberán poner a disposición dicha información a través de las tecnologías de la información.

REGISTRO OFICIAL: Órgano del Gobierno del Ecuador marca registrada de la Corte Constitucional.



TRIBUNAL CONTENCIOSO
ELECTORAL DEL ECUADOR

TRIBUNAL CONTENCIOSO
ELECTORAL DEL ECUADOR

RESOLUCIÓN: N° PLE-
TCE-530-29-08-2017

EXPÍDESE
EL REGLAMENTO
DE GESTIÓN TECNOLÓGICA
E INFORMÁTICA

PLE-TCE-530-29-08-2017

**EL PLENO DEL TRIBUNAL
CONTENCIOSO ELECTORAL**

Considerando

Que, el numeral 2 del artículo 16 de la Constitución de la República del Ecuador establece como derecho de las personas, en forma individual o colectiva, el acceso universal a las tecnologías de información y comunicación;

Que, el numeral 21 del artículo 66 de la Constitución de la República del Ecuador reconoce y garantiza a las personas el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; derecho que protege cualquier otro tipo o forma de comunicación;

Que, el artículo 217 de la Constitución de la República del Ecuador crea el Tribunal Contencioso Electoral, con jurisdicción nacional, personalidad jurídica propia y autonomía administrativa, financiera y organizativa;

Que, el numeral 3 del artículo 221 de la Constitución de la República faculta al Tribunal Contencioso Electoral para determinar su organización, formular y ejecutar su presupuesto;

Que, el artículo 227 de la Constitución de la República establece que la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación;

Que, el artículo 233 de la Constitución de la República del Ecuador señala que ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos;

Que, los numerales 10 y 11 del artículo 70 de la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia, facultan al Tribunal Contencioso Electoral para expedir la reglamentación necesaria para su funcionamiento, así como, determinar su organización, formular y ejecutar su presupuesto ordinario y el extraordinario para procesos electorales;

Que, el artículo 77 de la Ley Orgánica de la Contraloría General del Estado establece la obligación del Titular de la entidad de dirigir y asegurar la implantación, funcionamiento y actualización de los sistemas administrativos;

Que, el artículo 41 de la Ley Orgánica del Servicio Público, señala que la servidora o servidor público que incumpliere sus obligaciones o contraviniere las disposiciones de esa Ley, sus Reglamentos, así como las leyes y normativa conexa, incurrirá en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiese originar el mismo hecho;

Que, la Ley Orgánica de la Contraloría General del Estado, artículo 40, preceptúa que las autoridades, dignatarios, funcionarios y demás servidores de las instituciones del Estado, actuarán con la diligencia y empeño que emplean generalmente en la administración de sus propios negocios y actividades, caso contrario responderán, por sus acciones u omisiones, de conformidad con lo previsto en esa ley;

Que, el artículo 2 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos reconoce y otorga igual valor jurídico a los mensajes de datos que a los documentos físicos;

Que, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, artículo 148 y Disposición Transitoria Décima Tercera, determina a las entidades contratantes del sector público orden de prelación en la contratación pública relacionada a software y un plan de migración a software libre;

Que, el Reglamento General para la administración, utilización, manejo y control de los bienes y existencias del sector público, considera, en su artículo 4, la reglamentación interna para la administración, uso, control y destino de los bienes del Estado; y en los artículos 103 y 104, disposiciones para el registro y mantenimiento de equipos informáticos, hardware y software;

Que, las Normas de Control Interno de la Contraloría General del Estado, Grupo 410 Tecnologías de la Información y Grupo 500 Información y Comunicación, regulan la información y la comunicación y su soporte tecnológico informático, con necesaria referencia a un modelo de información de la organización que facilite la creación, uso y compartición de la misma y garantice su disponibilidad, integridad, exactitud y seguridad, sobre la base de la definición e implantación de los procesos y procedimientos correspondientes;

Que, la Norma de Control Interno 410-04 Políticas y procedimientos, determina a la Unidad de Tecnología de Información definir, documentar y difundir políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, considerándose temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información; así mismo, la incorporación de controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos; y, la implantación de procedimientos de supervisión de las funciones de tecnología de información;

Que, la Norma de Control Interno de la Contraloría General del Estado 410-14 Sitio web, servicios de internet e intranet, asigna a la Unidad de Tecnología de Información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos;



Que, la Norma de Control Interno 300-03 Valoración de los riesgos, determina "Se consideran factores de alto riesgo potencial los programas o actividades complejas... sistemas de información rediseñados... nueva tecnología, entre otros. La valoración del riesgo se realiza usando el juicio profesional y la experiencia";

Que, el artículo 19 del instructivo para el control de bienes del Tribunal Contencioso Electoral, dispone a la Unidad de Tecnología e Informática el plan anual de mantenimiento de los bienes tecnológicos, financiado con el pertinente presupuesto;

Que, los estándares del esquema gubernamental de seguridad de la información EGSi, emitido por la Secretaría Nacional de la Administración Pública, son en sentido técnico aplicables en los procesos de gestión del Tribunal Contencioso Electoral;

Que, se cuenta con las normativas expedidas en la materia por instituciones del sector público, con sujeción al marco legal aplicable, para sustentar políticas administrativas de gestión tecnológica e informática pertinentes en el Tribunal Contencioso Electoral;

Que, mediante Resolución de Pleno No. PLE-TCE-392-23-06-2015, publicada en el Registro Oficial Suplemento 552 de 27 de julio de 2015, se expide el Estatuto Orgánico de Gestión Organizacional por Procesos del Tribunal Contencioso Electoral;

Que, el Estatuto Orgánico de Gestión Organizacional por Procesos del Tribunal Contencioso Electoral, señala las atribuciones, responsabilidades y productos de la Unidad de Tecnología e Informática; y,

Que, es necesario establecer disposiciones internas para asegurar a los servidores del Tribunal Contencioso Electoral el acceso a la información y la comunicación, para el desarrollo de sus tareas y actividades habituales, a la par que garantizar el uso adecuado, transparente y efectivo de los recursos públicos asignados.

En ejercicio de sus atribuciones constitucionales y legales.

Resuelve:

Expedir el siguiente,

REGLAMENTO DE GESTIÓN TECNOLÓGICA E INFORMÁTICA PARA EL TRIBUNAL CONTENCIOSO ELECTORAL

**Capítulo I
DISPOSICIONES PRELIMINARES**

**Sección I
Objeto, ámbito, principios y obligatoriedad**

Art. 1.- Objeto.- El presente instrumento tiene por objeto reglamentar la administración, uso y acceso de los recursos tecnológicos e informáticos del Tribunal Contencioso

Electoral, mediante políticas y estándares correspondientes, a fin de alcanzar los objetivos institucionales en el contexto de autenticidad, confiabilidad, confidencialidad, integridad, auditabilidad, protección a la duplicación, no repudio, seguridad, disponibilidad y legalidad de la información que se produce, procesa, intercambia, reproduce y conserva en los procesos organizacionales.

Art. 2.- Ámbito.- Se sujetarán a la presente reglamentación los bienes de la infraestructura tecnológica; los servicios de red como son telefonía fija y móvil, internet, página web, correo electrónico, consultas de información legal; el sistema de gestión documental y las aplicaciones informáticas administrativas y jurisdiccionales desarrolladas y/o adquiridas; y, otras facilidades de base tecnológica informática con acceso habilitado a las y los servidores públicos del Tribunal Contencioso Electoral y/o terceros que interactúan con la Institución.

Art. 3.- Principios.- Las normas del presente instrumento se aplicarán bajo los principios de eficiencia, eficacia, calidad, buenas prácticas y responsabilidad.

Art. 4.- Obligatoriedad.- El cumplimiento del presente instrumento es obligatorio para todos los servidores del Tribunal Contencioso Electoral; así como también para terceros con quienes interactúan de manera habitual u ocasional y que además acceden a información sensible y/o a los recursos tecnológicos e informáticos de la Institución.

Las normas del presente Reglamento referidas a servidores del Tribunal Contencioso Electoral obligan en lo que corresponda a los demás usuarios. En caso de inobservancia se establecerá la responsabilidad a que hubiere lugar.

**Sección II
Política institucional**

Art. 5.- Directrices.- La gestión tecnológica e informática, en orden al cumplimiento de la misión, visión y objetivos estratégicos y operativos institucionales y, con la finalidad de garantizar la seguridad de la información del Tribunal Contencioso Electoral en los medios y el tiempo que su legitimidad y mérito requiera, se orientará por las directrices administrativas que se detallan a continuación; definiéndose y ejecutándose en conformidad los procesos, procedimientos y tecnologías en la medida en que generan, registran, utilizan, procesan, comparten, reproducen, recuperan, conservan y archivan información pública e información pública confidencial o reservada, en medio electrónico o escrito:

- La seguridad de la información preservará las características de autenticidad, confiabilidad, confidencialidad, integridad, auditabilidad, protección a la duplicación, no repudio, disponibilidad y legalidad de la información, verificadas previo análisis de riesgos y control de calidad.
- La gestión organizacional por procesos incorporará las tecnologías de la información y comunicación con la finalidad de asegurar la calidad, control, productividad,

4 - Miércoles 13 de septiembre de 2017 Edición Especial N° 84 - Registro Oficial

transparencia y continuidad del servicio público de justicia contencioso electoral; y, lo propio en los correspondientes procesos gobernantes, habilitantes, operativos y de seguimiento.

- c. Las tecnologías de la información y comunicación aplicadas cumplirán los estándares de seguridad de la información contemplados en el Esquema Gubernamental de Seguridad de la Información EGSI, en los términos establecidos por la normativa institucional interna del Tribunal Contencioso Electoral.
- d. La planificación estratégica efectuará las previsiones necesarias y la programación presupuestaria consultará el financiamiento del desarrollo de la infraestructura tecnológica e informática que soporta el modelo de información organizacional estructurado.
- e. El sistema de gestión documental administrativo, sobre la base del principio de coordinación del sector público, propenderá a la homologación con el sistema operativo en la Función Ejecutiva y la implementación del uso de la firma electrónica.
- f. El modelo de información de la organización reflejará una política de datos abiertos, salvo excepciones contempladas en norma legal competente, en especial las pertinentes a la gestión jurisdiccional respecto de reserva de la información conforme la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia, y la información pública clasificada confidencial a los efectos de la Ley Orgánica de Transparencia y Acceso a la Información Pública.
- g. La gestión tecnológica e informática en el Tribunal Contencioso Electoral se ajustará rigurosamente a la base legal de sus correspondientes procesos organizacionales, conforme los principios de legalidad, jerarquía normativa y competencia; y, en especial, a las normas pertinentes y aplicables de control interno emitidas por la Contraloría General del Estado, Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, su Reglamento General, Reglamento para la adquisición de software por parte de las entidades contratantes del sector público, Resoluciones del SERCOP, los principios de vigencia, transferencia y desagregación tecnológica, el Estatuto Orgánico de Gestión Organizacional por Procesos del Tribunal Contencioso Electoral, el presente Reglamento y más normativa aplicable en las instituciones del sector público.

Sección III Glosario de Términos

Art. 6.- Definiciones.- Para efectos de la aplicación de la presente reglamentación, se considerarán las siguientes definiciones:

1. Active Sync: Es un programa de sincronización de datos desarrollado por Microsoft para su uso con sus

sistemas operativos Microsoft Windows, proporciona a los usuarios de Microsoft Windows, una manera de transportar los documentos, calendarios, listas de contacto y correo electrónico entre la computadora de escritorio y un dispositivo móvil, como un PC de mano, teléfonos móviles, o cualquier otro dispositivo portátil que soporte el protocolo de ActiveSync. El protocolo usado para esto es Exchange ActiveSync.

2. Administración de riesgos: Comprende el proceso de control y minimización, o la completa eliminación, de los riesgos de seguridad que podrían afectar a la información de la Institución.

3. Auditabilidad: Asegura que todos los eventos de un sistema deben quedar registrados, permitiendo así su control posterior, ya sea en forma automática o manual.

4. Autenticidad: Propiedad que asegura el origen de la información y la identidad del emisor, misma que puede ser validada, de modo que se demuestre que es quien dice ser; en consecuencia, asegura la validez de la información en tiempo, forma y distribución; y, asimismo, garantiza el origen de la información al validar el emisor de ésta, para evitar suplantación de identidades.

5. Confiabilidad: La información debe ser adecuada para sustentar la toma de decisiones y la ejecución de las actividades propias de la Institución.

6. Confidencialidad: Es la propiedad de la información, por la que se garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma. La confidencialidad se entiende en el ámbito de la seguridad informática, como la protección de datos y de la información intercambiada entre un emisor y uno o más destinatarios frente a terceros.

7. Correo electrónico: Servicio de transmisión de mensajes a través de una red, los cuales pueden incluir archivos adjuntos.

8. Corresponsabilidad: Es la responsabilidad compartida entre dos o más sujetos, es decir que dicha responsabilidad es común entre quienes comparten una obligación o compromiso respecto de algo o de algún evento específico.

9. Unidad de Tecnología e Informática: Encargada de administrar y gestionar las tecnologías de información y comunicación dentro del Tribunal Contencioso Electoral.

10. Disponibilidad: Prevenir interrupciones no autorizadas/controladas de la dotación de recursos y servicios tecnológicos e informáticos. Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, siempre que lo requieran.

11. Equipo informático: Se refiere a todas las partes tangibles o físicas de un sistema informático.

12. Esquema Gubernamental de la Información, EGSI: Instrumento acordado por la Secretaría Nacional de la

Administración Pública [Registro Oficial Suplemento 88 de 25 de septiembre de 2013].

13. Evaluación de riesgos: Comprende las acciones realizadas para identificar y analizar las amenazas y vulnerabilidades relativas a la información y a los medios de procesamiento de la misma, así como la probabilidad de ocurrencia y el potencial impacto a las operaciones de la Institución.

14. GB o Gigabyte: Es la unidad de medida de cantidad de datos informáticos. Es un múltiplo del megabyte (MB), que equivale a 1024 MB.

15. Hardware: Se refiere a todas las partes tangibles de un sistema informático; sus componentes pueden ser eléctricos y electrónicos.

16. IMAP: Es un protocolo de aplicación de acceso a mensajes electrónicos almacenados en un servidor, mediante el cual se puede acceder al correo electrónico desde cualquier ordenador que posea una conexión a Internet, en su estricto nombre es el protocolo de acceso a los mensajes de internet (Internet Message Access Protocol).

17. Incidente de seguridad informática: Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizado de información; un impedimento en la operación normal de las redes de datos, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la política de seguridad de la información de la Institución.

18. Información: Se refiere a toda representación de conocimiento en forma de datos vinculados entre sí, generada utilizando letras, números, gráficos, cartografía, narrativa o audiovisuales; almacenada en cualquier medio, ya sea magnético, papel, pantallas de dispositivos electrónicos u otros.

19. Infraestructura tecnológica: Es el conjunto de hardware y software sobre el que residen los diferentes servicios que requieren estar en funcionamiento para dar soporte tecnológico en el desarrollo de las actividades de la Institución.

20. Integridad: La integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria; por consiguiente, salvaguarda la exactitud y la totalidad de la información y los métodos para su creación, recuperación y procesamiento.

21. Internet: Es una red mundial con millones de usuarios conectados o interconectados entre sí. Estos pueden intercambiar información y establecer distintos servicios tales como: visitar páginas de portales Web, correos electrónicos, charlar o chatear por medio del teclado en los salones creados para este servicio, entre otros.

22. Internet móvil inalámbrico: Es el servicio de acceso inalámbrico a la red internet mediante un modem USB que provee un ISP (Internet Service Provider) o a través de un equipo.

23. Intranet: Red local a la que se accede desde varias localizaciones geográficas distintas y que usa los mismos protocolos de comunicación que internet.

24. Legalidad: Garantizar el cumplimiento de las leyes, normas, Reglamentos o disposiciones.

25. Lista de distribución: Son listas de uso especial del correo electrónico que permite la distribución masiva de información entre múltiples servidores del Tribunal Contencioso Electoral mediante Internet a la misma vez.

26. Mantenimiento correctivo: Aquel que corrige los defectos observados en los equipamientos o instalaciones, es la forma más básica de mantenimiento y consiste en localizar averías o defectos y corregirlos o repararlos.

27. Mantenimiento preventivo: Es el destinado a la conservación de equipos o instalaciones mediante realización de revisión, mantenimiento y reparación periódica que garanticen su buen funcionamiento y fiabilidad. El mantenimiento preventivo se realiza en equipos en condiciones de funcionamiento.

28. MB o Megabyte: Es una unidad de medida de cantidad de datos informáticos. Es un múltiplo del byte u octeto, que equivale a 1000 bytes.

29. Modem USB: Es un dispositivo electrónico que se conecta en un computador para tener acceso al servicio de internet móvil inalámbrico.

30. No repudio: Característica de la información que asegura evitar que una entidad (persona o sistema informático) que haya interactuado con alguna información alegue ante terceros que no lo ha hecho.

31. Perfil de Riesgos Tecnológicos: Es la identificación, cuantificación, control y solución de las posibles amenazas que originan daños en los sistemas.

32. Periféricos: Equipos electrónicos tales como terminales, impresoras, dispositivos auxiliares de computadoras, entre otros.

33. Propietarios de la información: Son los responsables 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.

34. Protección a la duplicación: Característica de la información que asegura que una transacción sea realizada por una única vez, a menos que se especifique lo contrario.

35. Recurso Tecnológico: Es un medio que se vale de la tecnología para cumplir con su propósito.

36. Recurso Informático: Es cualquier componente físico o lógico de disponibilidad limitada en una computadora o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

37. Respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

38. Responsabilidad: Desarrollar sus funciones a cabalidad y en forma integral dentro de los plazos establecidos por sus superiores y por la ley.

39. Seguridad de la información: Preservación de las siguientes características de la información: confidencialidad, integridad, disponibilidad, autenticidad, auditabilidad, protección a la duplicación, no repudio, legalidad y confiabilidad.

40. Seguridades físicas: Es la precaución que debe tener el usuario del manejo, uso y cuidado de los equipos tecnológicos e informáticos.

41. Seguridades lógicas: Son las contraseñas de usuario, la prevención de contaminación por virus y otros programas que puedan causar daño en los equipos, en la información y otras facilidades.

42. Servidores: Personas que prestan sus servicios al Tribunal Contencioso Electoral y que en razón de sus funciones mantengan en su poder bienes, servicios y aplicaciones de carácter tecnológico de dotación oficial.

43. SIP: Tecnología IP, reemplazo de la telefónica convencional.

44. Sistema: Es el conjunto de partes interrelacionadas, hardware, software y de recurso humano que permite almacenar y procesar información.

45. Sistema de Gestión de Seguridad de la Información: Es un conjunto de políticas de administración de la información, que requiere del diseño, implementación y mantenimiento de un conjunto de procesos y procedimientos que permitan la gestión eficiente de la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de ésta, minimizando los riesgos. Un Sistema de Gestión de Seguridad de la Información debe ser eficiente a través del tiempo, adaptándose a los cambios de la Institución así como a los de su entorno.

46. Sistema de Información: Se refiere a un conjunto de recursos organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información que cumplen con determinadas características propias de la Institución, así como con procedimientos que pueden ser automatizados, manuales o mixtos.

47. SMTP: Es un protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos, en su estricto nombre es el protocolo simple de transferencia de correo (Simple Mail Transfer Protocol).

48. Software: El equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los

componentes necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

49. Software libre: Es la denominación del software que respeta la libertad de todos los usuarios que adquirieron el producto y, por tanto, una vez obtenido el mismo puede ser usado, copiado, estudiado, modificado y redistribuido libremente de varias formas, dependiendo del tipo de licenciamiento libre.

50. Software propietario: Este concepto se aplica a cualquier programa informático que no es libre o que sólo lo es parcialmente (semilibre), sea porque su uso, redistribución o modificación está prohibida, o sea porque requiere permiso expreso del titular del software.

51. Spam: Correo basura considerado no deseado.

52. Tecnologías de la información y comunicación: Se refiere a equipos de cómputo, aplicativos con desarrollo propio o adquiridos, medios de almacenamiento y comunicaciones, que en conjunto son operados por servidores del Tribunal Contencioso Electoral, o por un tercero, con el objetivo de procesar, almacenar y/o transmitir información para llevar a cabo una función propia de la Institución.

52. Terceros: Es toda persona ajena al vínculo jurídico existente entre el servidor o servidora del Tribunal Contencioso Electoral sin distinción del régimen laboral al que pertenezca el cual interactúa de manera habitual u ocasional con el servidor o servidora del Tribunal Contencioso Electoral o con la misma Institución; y, que además acceda a información sensible y/o a los recursos informáticos de la Institución.

53. TICs: Tecnologías de Información y Comunicaciones.

54. Uptime mensual: Es el tiempo que un determinado servicio está disponible en relación al tiempo de medición, en este caso un mes y vinculado estrictamente con un acuerdo de servicio.

56. Usuario: Es el servidor o un tercero que prestan servicios al Tribunal Contencioso Electoral y que utilizan las herramientas informáticas o tecnológicas asignadas a fin de ejecutar sus funciones en la Institución.

57. Vulnerabilidades: Debilidades de las tecnologías informáticas que pueden ser explotadas por una o más amenazas.

58. Webmail: Es un servicio que permite listar, desplegar y borrar vía un navegador web los correos almacenados en un servidor remoto, utilizando un protocolo de correo como IMAP o POP3.

59. WiFi: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica, lleva ese nombre de la sigla de la marca que la creó para referirse a una tecnología de redes inalámbricas. En el estricto nombre (WirelessFidelity) que literalmente significa fidelidad inalámbrica, es en sí un

conjunto de estándares y/o protocolos para redes que no requieren de cables y que funcionan en ciertos protocolos previamente establecidos.

60. Zimbra: Es un software libre, que incluye un servidor de correo electrónico.

Sección IV Propiedad y uso

Art. 7.- Régimen.- La infraestructura tecnológica asignada al servicio público de justicia contencioso electoral es de propiedad del Tribunal Contencioso Electoral.

La propiedad de la información pertinente a la gestión administrativa se verificará sin perjuicio del derecho de acceso a la información pública contemplado en la Ley Orgánica de Transparencia y Acceso a la Información Pública y con observancia de los derechos de propiedad intelectual regulados por el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.

Los equipos, sistemas, aplicaciones, servicios y en general recursos tecnológicos e informáticos solo podrán y deberán ser utilizados con fines lícitos y propios de las competencias del Tribunal Contencioso Electoral.

Sección V Comité de seguridad de la información

Art. 8.- Comité de Seguridad de la Información.- Con objeto de consulta, definición, informe y supervigilancia de políticas, normas y procedimientos relacionados con la seguridad de la información, su implantación y cumplimiento, se conformará el Comité de Seguridad de la Información del Tribunal Contencioso Electoral integrado por el Presidente del Tribunal o su Delegado, el Director Administrativo Financiero y el responsable de la Unidad de Tecnología e Informática, a fin de cumplir las siguientes responsabilidades:

- Proponer: reformas al presente Reglamento, normas complementarias o solicitará a la Máxima Autoridad la aprobación de instructivos, guías u otros instrumentos relacionados con la seguridad de la información en el Tribunal Contencioso Electoral.
- Definir e informar la política y normas institucionales en materia de seguridad de la información, gestionar su aprobación por parte del órgano competente y supervigilar el cumplimiento por parte de los servidores de la Institución.
- Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes y evaluar los incidentes relativos a la seguridad de la información.
- Conocer y recomendar iniciativas para incrementar la seguridad de la información.
- Consultar e informar metodologías y procesos específicos relativos a la seguridad de la información

y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

- Promover la difusión y apoyo a la seguridad de la información dentro de la Institución.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la Institución frente a incidentes de seguridad imprevistos.
- Velar por la provisión de recursos económicos, tecnológicos y humanos necesarios para la gestión de la seguridad de la información.
- Solicitar la aprobación de actos administrativos y normativos conducentes a los órganos competentes del Tribunal Contencioso Electoral.

Integrará además el Comité de Seguridad de la Información el Director de Auditoría Interna, con voz pero sin voto con fines de asesoría.

El Comité, convocado por el Administrativo Financiero o su delegado, establecerá la normativa para su funcionamiento.

Art. 9.- Unidad de Tecnología e Informática.- El responsable de la Unidad de Tecnología e Informática será responsable de la seguridad de la información en la Institución, con las siguientes atribuciones y responsabilidades que cumplirá en forma concordante con las asignadas en el Estatuto Orgánico de Gestión Organizacional por Procesos, las Normas de Control Interno de la Contraloría General del Estado y demás normativa pertinente:

- Asegurar la aplicación de los estándares de seguridad de la información establecidos en el presente Reglamento, plan informático estratégico de tecnología, plan de contingencia tecnológica, modelo de información organizacional y más productos/servicios de la Unidad de Tecnología e Informática, con enfoque de gestión de la calidad y administración de riesgos.
- Verificar y vigilar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.
- Monitorear las necesidades de capacidad tecnológica de los sistemas en operación y proyectar las futuras demandas de esta capacidad para soportar potenciales amenazas a la seguridad de la información que procesan.
- Solicitar la reunión del Comité de Seguridad de la Información, cuando la situación lo amerite, actuar en calidad de Secretario, llevar registros de asistencia y actas de las reuniones.
- Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones y verificar su cumplimiento; de manera que, no afecten la seguridad de la información.

- f. Informar criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de pruebas antes de su aprobación definitiva.
- g. Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas, equipamiento y verificar su correcta implementación, asignando responsabilidades.
- h. Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones y adoptar o solicitar medidas correctivas.
- i. Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a través de las redes de comunicación de la Institución.
- j. Implementar los controles de seguridad definidos.
- k. Gestionar los incidentes de seguridad de la información de acuerdo al procedimiento aprobado por el Comité de Seguridad de la Información.
- l. Controlar los mecanismos y canales de distribución y difusión de información dentro y fuera de la Institución.
- m. Registrar la documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
- n. Administrar los medios técnicos necesarios para permitir la segregación o separación sistemática de los ambientes de procesamiento.
- o. Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento e informes impresos y verificar la eliminación o destrucción segura de los mismos, cuando proceda.
- p. Administrar y controlar la obtención de copias de resguardo de información, así como la prueba periódica de su restauración.
- q. Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
- r. Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios en los mismos.
- s. Coordinar la gestión de eventos de seguridad con otras entidades gubernamentales.
- t. Coordinar las actividades conducentes, asignar responsabilidades por escrito al personal de la Unidad

de Tecnología e Informática y solicitar a los órganos competentes de la Institución los actos o autorizaciones necesarios.

- u. Otras atribuciones y responsabilidades establecidas en el presente Reglamento y las que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas y no se encuentren asignadas a un superior jerárquico.

Capítulo II ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS

Sección I Asignación, control y mantenimiento de los recursos informáticos

Art. 10.-Asignación por entrega.- Las entregas, revisiones y/o cambios de los equipos, sistemas y recursos informáticos serán requeridas a la Dirección Administrativa Financiera, quien dispondrá a la Unidad de Tecnología e Informática para que, a través de un técnico de su área, proceda con lo solicitado y comunique al titular de la Unidad de Servicios Institucionales para que elabore la respectiva acta de entrega recepción.

La entrega de los equipos o sistemas informáticos la realizará la Dirección Administrativa Financiera con la colaboración de un técnico de la Unidad de Tecnología e Informática, previa suscripción de la respectiva acta de entrega recepción, a la que se acompañará una copia del manual de uso del bien, equipo o sistema para su correcta utilización, cuando el caso lo amerite.

Art. 11.- Custodia.- Los servidores a quienes se autorice la entrega-recepción de los bienes, equipos y sistemas informáticos, serán responsables de su uso, custodia y buena conservación de conformidad a las normas del Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, el presente Reglamento y la normativa institucional.

Cualquier novedad que se presentare con relación a los bienes, equipos o sistemas, será inmediatamente notificada por el custodio a la Unidad de Tecnología e Informática, sin perjuicio del cumplimiento de los procedimientos establecidos en otras normas aplicables.

Art. 12.- Registro y control.- La Dirección Administrativa Financiera será responsable del registro, custodia y administración de los bienes y equipos informáticos; la Unidad de Tecnología e Informática será responsable del control y monitoreo del buen uso, para lo cual:

- a) Identificará y verificará periódicamente todos los bienes tecnológicos y de comunicaciones en un registro del que constará el historial, estado actual, inventario físico y lógico, coordinará una conciliación con los registros contables financieros, registrará a los custodios y mantendrá un respaldo de las actas de entrega recepción.
- b) Comprobará el correcto funcionamiento de los bienes, equipos y sistemas informáticos de la Institución.



c) Comunicará a la Dirección Administrativa Financiera o a quien corresponda cualquier novedad que se presente respecto a los bienes, equipos y sistemas informáticos de la Institución.

d) Cumplirá las atribuciones y responsabilidades que el presente Reglamento asigna a la Unidad de Tecnología e Informática.

La Unidad de Tecnología e Informática cumplirá lo indicado en los numerales que anteceden, con observancia de las disposiciones de control constantes del artículo 104 del Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, codificación publicada en el Registro Oficial Suplemento 888 de 23 de noviembre de 2016.

Art. 13.- Mantenimiento.- La Unidad de Tecnología e Informática elaborará un plan de mantenimiento preventivo y correctivo de los bienes, equipos y sistemas informáticos que dispone la Institución, contemplando en la planificación institucional los recursos necesarios para su contratación.

La Unidad de Tecnología e Informática se encargará de gestionar los mantenimientos planificados con hora de inicio, fin, impacto y responsables, y pondrá previamente en conocimiento de los servidores custodios de los bienes informáticos, para que los entreguen o permitan su mantenimiento.

En caso de producirse daños o desperfectos en los equipos, sistemas o recursos informáticos, el servidor responsable y custodio de los mismos informará lo sucedido, oportunamente y por escrito, a la Unidad de Tecnología e Informática para que se tomen los correctivos necesarios o en su defecto se solicite la respectiva reparación o cambio de los mismos, según corresponda.

La Unidad de Tecnología e Informática establecerá controles apropiados para realizar mantenimientos programados y emergentes; y, conservará los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas generadas.

Los mantenimientos se realizarán únicamente con personal autorizado y calificado.

El plan de mantenimiento se ajustará a las disposiciones del artículo 103 del Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, codificación publicada en el Registro Oficial Suplemento 888 de 23 de noviembre de 2016; y a las disposiciones del principio de vigencia tecnológica que establece el capítulo III del Título III de la codificación y actualización de las resoluciones emitidas por el Servicio Nacional de Contratación Pública, de 31 de agosto de 2016.

Art. 14.- Devolución.- Las devoluciones de los equipos o sistemas informáticos por cualquier razón que esta sea, tendrá que realizarse de acuerdo al siguiente procedimiento:

a. Los bienes o equipos informáticos tienen que ser entregados por parte del custodio al responsable o delegado de la Unidad de Tecnología e Informática,

quien en coordinación con Servicios Generales procederá a revisar el estado y condiciones del bien, para con posterioridad suscribir la o las actas de devolución y se actualizará la hoja de vida del bien.

b. En el caso de encontrar novedades en la devolución de los equipos se reportará a la Dirección Administrativa Financiera para que tome los correctivos o acciones pertinentes.

c. En caso que la devolución del bien se deba a motivos de ausencia temporal, definitiva o cambios al interior de la Institución del servidor custodio, en forma previa este deberá entregar a su jefe inmediato y a la Unidad de Tecnología e Informática un respaldo magnético completo de la información constante en el mismo, esta acción será respaldada por la firma de un acta entrega de información digital, la cual tendrá que ser firmada por el funcionario saliente, un servidor de la Unidad de Tecnología e Informática y el jefe inmediato superior.

d. El respaldo de la información será de responsabilidad de la Unidad de Tecnología e Informática y del propietario de la información, para lo cual se determinarán los procedimientos de resguardo y contención de la información en el Instructivo que aprobará la máxima autoridad a petición del Comité de Seguridad de la Información.

e. La Unidad de Tecnología e Informática deberá proceder a formatear y tener listos los equipos para asignarlos a nuevos servidores que así lo requieran.

Sección II

Procedimiento de creación, modificación y eliminación de usuarios

Art. 15.- Procedimiento.- A fin de garantizar la seguridad de la información contenida en los sistemas informáticos de la Institución, para crear un nuevo usuario, el mismo tiene que ser aprobado por la Dirección Administrativa Financiera, quien autorizará los perfiles de usuario y atribuciones, según sea el caso, y dispondrá a la Unidad de Tecnología e Informática dicha creación, modificación o eliminación previa comunicación por escrito.

No se crearán cuentas anónimas o de invitado.

Art. 16.- Eliminación.- Para proceder a eliminar un usuario, la Unidad de Administración de Talento Humano tiene la obligación de informar y enviar dicho pedido para su aprobación a la Dirección Administrativa Financiera, quien dispondrá a la Unidad de Tecnología e Informática la eliminación del usuario en los sistemas en los cuales se registró, teniendo además que respaldar la información del servidor, según sea el caso.

La Unidad de Tecnología e Informática no almacenará información en los servidores institucionales referente a perfiles de usuario (Mis documentos, Escritorio, etc.), motivo por el cual, la responsabilidad de la información que se genere y custodie en cada equipo institucional será directamente del jefe inmediato del servidor que cese en sus funciones. La Unidad de Tecnología e Informática



dará soporte técnico, de ser el caso, para el respaldo de la información existente que reposa en el computador, sin discretización de la misma.

Art. 17.- Contraseña de Usuarios.- Para todo aspecto referente al manejo de contraseñas deberá ser aplicado el artículo 54 del presente instrumento, haciendo hincapié que las contraseñas administradas en los servicios de correo electrónico y de perfiles de equipo son centralizadas y encriptadas en el servidor de cómputo donde reside el servicio de Directorio Activo (Active Directory), herramienta que es continuamente actualizada para mitigar o reducir problemas de seguridad. En caso de emergencia de seguridad el personal técnico tendrá la autorización para solicitar el cambio de contraseñas sin previo aviso, de forma inmediata y una vez mitigado el problema entregará un informe de los acontecimientos suscitados.

Art. 18.- Manejo de Contraseñas.- Todo servidor del Tribunal Contencioso Electoral o tercero desde el momento que ingrese a prestar sus servicios en la Institución, deberá firmar un "Acuerdo de Confidencialidad", el mismo que incluirá responsabilidad en el uso de claves y medios electrónicos institucionales, lo que determinará que son los únicos responsables de todas las actividades realizadas con sus claves asignadas para el servicio de telefónica fija o celular a su cargo, cuentas de acceso a su buzón de correo electrónico, servicio de Internet que hayan sido entregados como herramientas de trabajo.

Art. 19.- Utilización excepcional de cuentas de usuario.- La utilización de las cuentas de usuario no deben proporcionarse a personas que no sean servidores públicos del Tribunal Contencioso Electoral, a excepción de aquellos que estén debidamente autorizados por la Máxima Autoridad.

Sección III

Seguridad, protección y cuidado

Art. 20.- Seguridad.- A fin de garantizar la seguridad de los bienes, equipos, sistemas y recursos informáticos de la Institución todo usuario observará las siguientes normas:

- Será responsabilidad de la Unidad de Tecnología e Informática gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
- Definir claramente el personal responsable de la administración de los permisos de acceso a la información por cada Despacho de Juez, Dirección o Unidad.
- Definir el administrador de accesos que debe controlar los perfiles y roles.
- Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (precautelando la debida confidencialidad).

- La Unidad de Tecnología e Informática tendrá la obligación de recomendar y controlar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales difíciles de descifrar, es decir, que cumplan una complejidad media o alta.
- La Unidad de Tecnología e Informática gestionará el cambio periódico de contraseñas de los usuarios.
- Evitar contraseñas en blanco o que vienen por defecto según el sistema del fabricante del producto, puesto que son fácilmente descifrables.
- La Unidad de Tecnología e Informática tendrá la obligación de generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología.
- Todo usuario registrado será responsable de proteger su nombre de usuario, contraseña y demás seguridades que sean implementadas por la Institución, de cualquier acceso no autorizado, para lo cual considerará que las cuentas institucionales no se pueden compartir ni delegar y que debe proteger su contraseña y cambiarla regularmente.
- Tener especial cuidado en el uso y manejo de las claves y seguridades empleadas para acceder a los servicios tecnológicos de la Institución.
- Se prohíbe el uso no autorizado de un nombre de usuario o claves de un usuario distinto al propiamente registrado.
- En caso de la utilización de un nombre de usuario no autorizado, el afectado comunicará inmediatamente tal hecho a la Unidad de Tecnología e Informática, a fin de adoptar los correctivos que sean del caso.
- Todo usuario respetará las claves, seguridades o contraseñas de los demás usuarios y funcionarios de la Institución, que por el ejercicio de sus funciones pudieren llegar a su conocimiento, como parte de su trabajo o de forma accidental. Si se diera algún caso de obtención de contraseña de otro usuario se deberá comunicar este evento a la Unidad de Tecnología e Informática, a fin de adoptar los correctivos que sean del caso.
- Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie fecha, creación, eliminación, suspensión, activación o eliminación del acceso al igual que cada usuario dispondrá de los servicios de acceso que han sido asignados.
- La Unidad de Tecnología e Informática está en la obligación de mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio, software o sistema operativo, sistema de gestión de base de datos y aplicaciones.
- Evidenciar documentadamente que cada activo de información tecnológica tenga definido los niveles de

acceso basado en perfiles y permisos, a fin de determinar qué privilegios se deben asignar según las actividades de los usuarios y las necesidades de la Institución y sus funciones.

- q. No se podrá modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos; en este sentido, todo usuario interno o externo respetará las políticas implantadas por la Institución referentes a la asignación y privilegios de acceso a los servicios tecnológicos.
- r. El acceso a los servicios con privilegios especiales se realizará previa autorización de la Máxima Autoridad o de la Dirección Administrativa Financiera y será de responsabilidad de la Unidad de Tecnología e Informática mantener actualizado el listado de los funcionarios con acceso a dichos servicios.
- s. No se podrá modificar, alterar, sustituir, remplazar, bloquear, restringir o almacenar información institucional con el propósito de impedir que un usuario pueda acceder o disponer de ella sin la debida autorización.
- t. En caso de que algún usuario asigne contraseñas o codifique la información institucional a fines de evitar que otros usuarios puedan acceder o disponer de ella, éste facilitará la información necesaria para lograr el acceso a los archivos o en su defecto se impondrán las medidas disciplinarias que correspondan frente a este hecho. La Institución, a través de la Unidad de Tecnología e Informática, estará facultada para decodificar la misma o restituirla a su condición original y reportar cualquier novedad sobre su tratamiento.
- u. La información generada por los servidores en el ejercicio de sus funciones o actividades laborales en la Institución deberá permanecer siempre almacenada en los equipos informáticos asignados por la Unidad de Tecnología e Informática. Está prohibido el almacenamiento en equipos o dispositivos que no reposen o sean de propiedad del Tribunal Contencioso Electoral, salvo el caso de que se traten de respaldos de información personal.
- v. El acceso a las oficinas, infraestructura, bienes, equipos y sistemas informáticos que dispone la Institución será coordinado únicamente por intermedio de la Unidad de Tecnología e Informática, a través de los servidores que pertenecen a esta unidad o por autorización de la Máxima Autoridad o la Dirección Administrativa Financiera. Los demás servidores podrán acceder a los mismos únicamente con el acompañamiento o aprobación de la Unidad de Tecnología e Informática.
- w. Queda prohibido congestionar enlaces de comunicaciones o sistemas informáticos mediante la ejecución de programas maliciosos o de reproducción de radio, video, transferencia de archivos o programas que sean para uso personal y que no sean necesarios para el cumplimiento de las labores institucionales.

- x. La información institucional que se genere, utilice, procese, comparta y almacene en cualquier medio electrónico o escrito, clasificada como pública o pública confidencial o reservada, deberá manejarse y utilizarse conforme lo determina el presente Reglamento u otros instrumentos institucionales, a fin de definir por parte de la Unidad de Tecnología e Informática los procesos, procedimientos y medios tecnológicos que permitan garantizar la confidencialidad, integridad y disponibilidad de esa información institucional, en los medios y el tiempo que su legitimidad lo requiera.
- y. La Unidad de Tecnología e Informática establecerá protocolos de uso, manejo y seguridad de la información institucional, con la finalidad de garantizar y precautelar la debida confidencialidad y reserva de la misma.

Art. 21.- Equipos periféricos.- A fin de garantizar la protección y cuidado de los bienes o equipos periféricos (terminales, impresoras, dispositivos auxiliares para computadoras, etc.), todo usuario observará las siguientes normas:

- a. Únicamente el personal autorizado por la Unidad de Tecnología e Informática podrá manipular, sustituir, instalar y configurar los equipos tecnológicos, de computación o sistemas informáticos.
- b. En caso de que el usuario detecte problemas en el funcionamiento de los bienes, equipos o sistemas informáticos de la Institución, deberá notificar inmediatamente a la Unidad de Tecnología e Informática para que se proceda con la revisión de los mismos, a fin de que se tomen los correctivos del caso o se envíen para la respectiva revisión o reparación, según corresponda.
- c. No se podrá tener o consumir alimentos ni bebidas en las áreas de trabajo donde se encuentren localizados los bienes, equipos o sistemas informáticos.
- d. Cualquier movimiento, traspaso o reubicación de los bienes o equipos informáticos de la Institución, así como de sus periféricos deberá ser coordinado con el personal de la Unidad de Tecnología e Informática, para lo cual se solicitará a la Dirección Administrativa Financiera la elaboración del documento de traspaso correspondiente.
- e. Al finalizar sus labores diarias, cada usuario deshabilitará su clave de acceso del terminal o computadora y apagará todos los equipos electrónicos en su área de trabajo, o cuando así se lo requiera.

Sección IV Equipos de reproducción

Art. 22.- Utilidad.- El uso de equipos de reproducción como impresoras, copiadoras, escáneres, etc., serán única y exclusivamente para fines estrictamente laborales o relacionados con las funciones y actividades desempeñadas en la Institución; se imprimirá los documentos cuando fuere estrictamente necesario.



Art. 23.- Uso racional.- Será obligatorio el uso adecuado, racional y estrictamente necesario de los equipos de reproducción, al momento de realizar la impresión o copiado de documentos, para lo cual la Unidad de Tecnología e Informática realizará un seguimiento, control y llevará un reporte de las impresiones realizadas por cada una de las áreas o unidades, con el fin de dar cumplimiento a esta disposición.

Art. 24.- Consumibles.- Los consumibles de las impresoras o copiadoras deberán ser cambiados o remplazados únicamente por el personal de la Unidad de Tecnología e Informática, previa solicitud del área requirente y constatación del agotamiento de los mismos, entre otros: toners, cintas de impresora zebra, rodillos, fotoconductores de impresoras multifunción y aquellos que de acuerdo al avance tecnológico sean considerados como tales.

Art. 25.- Daños y desperfectos.- En caso de producirse daños o desperfectos en los equipos de reproducción, el servidor responsable y custodio de los mismos informará lo sucedido oportunamente y por escrito a la Unidad de Tecnología e Informática para que se tomen los correctivos necesarios o en su defecto se solicite la respectiva reparación y cambio de estos.

Sección V Software

Art. 26.- Adquisición de software.- Previo a iniciar el proceso de contratación, toda unidad requirente deberá solicitar a la Unidad de Tecnología e Informática la validación de las especificaciones técnicas del caso.

Todo software propietario que se utilice en los equipos informáticos del Tribunal Contencioso Electoral deberá ser adquirido a nombre de la Institución y contar obligatoriamente con su licencia legal.

Art. 27.- Contratos con terceros.- Para la adquisición de equipos informáticos de escritorio o equipos portátiles, equipos de impresión, equipos de telecomunicaciones y software de terceros, se contemplará una cláusula en el respectivo contrato que establezca el procedimiento para la obtención de datos, programas fuentes, manuales y documentación asociada por imprevistos que pudiera sufrir el proveedor y que provoquen la culminación de sus servicios, procedimiento que deberá contemplarse en los términos de referencia elaborados por el área requirente del bien o servicio.

Art. 28.- Software recibido para prueba.- En caso que la Institución reciba software de terceros para ser probados y evaluados por el Tribunal Contencioso Electoral, se deberá suscribir un acta en donde consten las funcionalidades generales del sistema, el cual se implementará en un ambiente tecnológico alternativo al ambiente final o de producción institucional.

Art. 29.- Instalación de software.- La Unidad de Tecnología e Informática es responsable de la homologación inicial, instalación y/o eliminación de cualquier tipo de software en los equipos centralizados de procesamiento y/o

en cualquiera de los equipos conectados o no a la red de datos del Tribunal Contencioso Electoral.

Art. 30.- Desarrollo interno de software.- Todo software desarrollado por la Unidad de Tecnología e Informática será de propiedad del Tribunal Contencioso Electoral, para lo cual la Dirección de Asesoría Jurídica deberá registrarlo a nombre de la Institución, conforme las disposiciones de propiedad intelectual vigentes.

Art. 31.- Transferencia y donaciones a terceros.- Toda transferencia a terceros de software desarrollado por el Tribunal Contencioso Electoral será autorizada por la Máxima Autoridad y contará con el correspondiente respaldo legal.

En toda donación de equipos informáticos se identificarán detalladamente todos los recursos de software que se incluyen en la operación.

Art. 32.- Control de licencias.- La Unidad de Tecnología e Informática elaborará un inventario de las versiones de software instaladas en todos los equipos informáticos del Tribunal Contencioso Electoral, el cual será actualizado periódicamente de manera trimestral.

Capítulo III SERVICIO DE TELEFONÍA IP

Sección I Uso del servicio

Art. 33.- Utilidad.- El servicio de telefonía IP es una herramienta de trabajo institucional, por lo que todo servidor o servidora deberá dar un uso adecuado a este servicio, precautelando que el tiempo utilizado sea el estrictamente necesario para el cumplimiento de sus labores y objetivos de la Institución.

Art. 34.- Habilitación.- El servidor no requerirá de claves, códigos o autorizaciones especiales para el uso de llamadas permitidas (locales, provinciales, regionales y llamadas a líneas gratuitas) a excepción de las llamadas a celular e internacional. En caso de que se detecte el uso anormal de las claves entregadas, con el fin de adoptar medidas pertinentes, previa autorización de la Máxima Autoridad, se deberá recabar la información necesaria solicitando los registros de llamadas a la Unidad de Tecnología e Informática, justificando el motivo de dicha solicitud.

Art. 35.- Prohibiciones.- Se prohíbe a los servidores del Tribunal Contencioso Electoral:

- Mover o crear extensiones con o sin clave.
- Mover los teléfonos a unidades o despacho distintos a los entregados.
- Difundir y utilizar las claves de acceso, entregadas únicamente a los servidores autorizados por la Máxima Autoridad.
- Utilizar este servicio para actividades ajenas a la Institución.

**Sección II
Control**

Art. 36.- Consumo y debido uso.- La Unidad de Tecnología e Informática realizará un control trimestral del servicio, uso y consumo de la telefonía IP, verificando además que el uso de las claves asignadas a servidores específicos no tengan un acceso diferente al autorizado; y, de ser el caso, podrá limitar el acceso a dichas claves, previa autorización del titular de la Dirección Administrativa Financiera conforme a las necesidades del servidor.

Art. 37.- Supervisión.- La Dirección Administrativa Financiera vigilará, sobre la base de un reporte mensual de la Unidad de Tecnología e Informática, que los gastos por consumo de telefonía IP, especialmente los servicios de larga distancia nacional e internacional que demandan cargos por interconexión con otras operadoras telefónicas, se reduzcan al mínimo indispensable, tendiendo siempre a la utilización óptima del servicio e informando de cualquier anomalía a la Máxima Autoridad o su delegado, a fin de que establezcan los correctivos necesarios.

Art. 38.- Listado.- La Dirección Administrativa Financiera asignará y mantendrá actualizados los listados de los responsables de las extensiones y claves, de ser el caso, de la telefonía IP, y realizará el monitoreo del uso y el tipo de accesos requeridos y autorizados.

Art. 39.- Verificación.- La Unidad de Administración de Talento Humano notificará a la Unidad de Tecnología e Informática los cambios de puestos, permisos, traslados y cesación de funciones de los servidores del Tribunal Contencioso Electoral, a fin de proceder con las medidas necesarias que permitan el control de las claves, abiertas al servicio de telefonía IP

La notificación a la que se refiere el inciso anterior no podrá ser superior a las 48 horas de expedido el acto administrativo en cualquiera de los casos determinados en el inciso precedente.

**Sección III
Seguridades**

Art. 40.- Autorización.- La Dirección Administrativa Financiera, previa autorización de la Máxima Autoridad o su delegado, dispondrá a la Unidad de Tecnología e Informática asignar y entregar una clave personal para realizar llamadas a celular e internacionales a los servidores designados para tal efecto, quienes serán los únicos responsables del manejo de la misma.

Art. 41.- Actualización.- Las claves de acceso se actualizarán periódicamente según lo determine la Dirección Administrativa Financiera y cuando lo solicite el usuario.

**Sección IV
Acciones correctivas**

Art. 42.- Suspensión.- La Dirección Administrativa Financiera podrá suspender los accesos a los servicios de telefonía IP en los casos de solicitud motivada y expresa del servidor responsable de la clave, por considerarse innecesario el servicio o por exceso no justificado del consumo, así como por disposición expresa de las autoridades de la Institución.

Art. 43.- Responsabilidad.- De comprobarse que el servicio de telefonía IP está siendo utilizado por el servidor en actividades ajenas a las del Tribunal Contencioso Electoral, se ejercerá por parte de la Institución el derecho a cobrarle los valores incurridos, previo informe motivado de la Unidad de Tecnología e Informática.

Art. 44.- Acceso no autorizado.- De encontrarse o verificarse el servicio telefónico con acceso no autorizado, el custodio de la clave deberá explicar su indebida utilización a fin de que la Unidad de Tecnología e Informática tome las medidas o acciones preventivas o correctivas que se ameriten.

Art. 45.- Capacitación.- La Unidad de Administración de Talento Humano conjuntamente con la Unidad de Tecnología e Informática brindará capacitación a todo el personal y en particular al personal encargado de atender llamadas telefónicas respecto del uso de los dispositivos, la cortesía al público, amabilidad y diligencia con que deben hacerlo, con el objeto de precautelar los recursos y la imagen institucional.

**Capítulo IV
SERVICIO DE CORREO ELECTRÓNICO**

**Sección I Uso
del servicio**

Art. 46.- Utilidad.- Este servicio deberá utilizarse exclusivamente para el ejercicio de las funciones propias de cada servidor del Tribunal Contencioso Electoral, por lo tanto se prohíbe el envío de mensajes individuales o en cadena ajenos al ámbito de gestión de la Institución.

Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información o archivo adjunto al mismo.

Art. 47.- Medidas de seguridad.- Son todos aquellos mecanismos tecnológicos e informáticos que se aplicarán a todo el servicio de correo electrónico institucional en la red interna y externa que es utilizada por servidores del Tribunal Contencioso Electoral para el envío y recepción de mensajes electrónicos, como herramienta para desarrollo de las actividades que realizan en el marco de sus funciones. Estas medidas tienen por finalidad evitar riesgos en la transmisión de información mediante el correo electrónico institucional provocados por un inadecuado manejo, para lo cual se deberán aplicar las siguientes normas:

- a. Las cuentas de correo electrónico institucional podrán ser monitoreadas y respaldadas por parte de la Unidad de Tecnología e Informática para efectos de supervisión administrativa y determinar el mal uso de la cuenta de ser el caso. Los mensajes deben mantenerse en carpetas personales, lo que permitirá archivar la información de acceso exclusivo del usuario, para ello se definirá un límite de espacio máximo a destinarse para este efecto sin que dicha información pueda ser compartida con otros usuarios.
- b. La o las cuentas de correo electrónico institucional deberán estar asociadas a una única cuenta de usuario, lo cual realizará la Unidad de Tecnología e Informática.
- c. Toda la información debe ser gestionada de forma centralizada y no en las estaciones de trabajo de los usuarios, como una medida de seguridad de la información, lo cual realizará la Unidad de Tecnología e Informática y se informará de su cumplimiento a las unidades de la Institución.
- d. El correo electrónico contará con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error. La Unidad de Tecnología e Informática, de ser el caso, informará de los errores presentados en el envío del mensaje a las unidades de la Institución.

Art. 48.- Conexión en red.- El acceso al correo electrónico únicamente se realizará a través un navegador Web sin necesidad de realizar descargas de mensajes al propio ordenador y por medio de protocolos de sincronización POP3 e IMAP, excepto para la gestión de correos en dispositivos móviles y tabletas. No se autoriza el uso de cualquier software gestor de correo electrónico en los computadores institucionales diferente a un navegador Web.

Sección II Responsabilidades

Art. 49.- Responsabilidad del usuario.- Son responsabilidades del usuario:

- a. Administrar la información respecto a la recepción de correos al destinatario de la información.
- b. Verificar la carpeta de correos spam y eliminarlos directamente sin abrirlos en caso de existir.
- c. Verificar mensajes de alerta de exceso del tamaño de su buzón.
- d. Notificar a la Unidad de Tecnología e Informática en caso de permisos, vacaciones o ausencia temporal para establecer el respectivo mensaje de notificación a los destinatarios de correo.
- e. Depurar el buzón de su correo, con el fin de no saturar el espacio asignado a su cuenta de correo.

- f. En caso de llegar al límite del tamaño de su buzón, notificar a la Unidad de Tecnología e Informática para realizar un respaldo de la cuenta e inmediatamente el usuario procederá a eliminar los correos que crea pertinente en fin de liberar espacio en la cuenta.
- g. Todo usuario es responsable por el uso y manipulación de los mensajes con origen desconocido y asume la responsabilidad por las consecuencias que pueda ocasionar a los recursos tecnológicos e informáticos la ejecución de los archivos adjuntos. En estos casos, no debe contestar dichos mensajes y enviará una copia a la Unidad de Tecnología e Informática para que efectúe el seguimiento y análisis correspondiente, o en su defecto eliminarlos.

Art. 50.- Responsabilidad de la Unidad de Tecnología e Informática.- Son sus responsabilidades:

- a. Mantener la seguridad por medio de un antivirus actualizado y análisis de tráfico generado dentro de la Institución.
- b. Asegurar la descarga de correos antiguos a un repositorio local para la limpieza del buzón.
- c. Generar reportes de uso de correo, de acuerdo con la petición de las autoridades, en razón de la propiedad intelectual de la Institución respecto de la información contenida en los equipos y correo electrónico. Estos reportes se realizarán de conformidad con las disposiciones legales vigentes.

Sección III Seguridades

Art. 51.- Pie de firma.- El formato de pie de firma en los correos electrónicos mantendrá el formato de imagen (jpeg) asignado por la Unidad de Comunicación Social a cada uno de los servidores y contendrá necesariamente: nombres y apellidos completos, denominación del cargo que ocupa, descripción del Despacho, Dirección o Unidad donde labora, nombre y teléfono de la Institución y dirección electrónica del sitio Web Institucional. Cada servidor es responsable de mantener y difundir en sus correos la firma actualizada. No se podrá incluir firmas personalizadas.

Art. 52.- Permisos de acceso.- Todos los servidores del Tribunal Contencioso Electoral, así como terceros que interactúan con la Institución, tendrán permisos de acceso única y exclusivamente a los recursos informáticos para los que han sido debidamente asignados por autoridad competente; en este contexto, las actividades descritas a continuación se desarrollarán de la siguiente manera:

- a. Las listas de distribución públicas serán creadas solamente por la Unidad de Tecnología e Informática, conforme a lo señalado en el Estatuto Orgánico de Gestión de Procesos del Tribunal Contencioso Electoral y a los requerimientos de cada una de las unidades que lo conforman.
- b. En caso de necesitar la creación o modificación de una lista de distribución se deberá remitir un correo

electrónico a la Unidad de Tecnología e Informática, solicitando lo correspondiente.

- c. El acceso a las listas de distribución solo se realizará desde cuentas de correo internas de la Institución que tengan la autorización debida por parte del órgano competente.
- d. Los correos enviados hacia las listas de distribución deben tener archivos adjuntos con un tamaño máximo de 6 MB y serán enviados con un tiempo promedio de una hora y media entre cada uno de los envíos masivos.
- e. Las cuentas de correo electrónico institucional permitirán el envío y la recepción de mensajes asociados a esta dirección única "nombre.apellido@tce.gob.ec". Para acceder a una cuenta de correo se requiere de la dirección única y contraseña, las cuales son almacenadas en un repositorio de ACTIVE DIRECTORY. Estas contraseñas serán gestionadas directamente por el servidor luego de una asignación con clave temporal por parte de la Unidad de Tecnología e Informática y su uso se limitará al cumplimiento de las funciones institucionales.
- f. La cuenta del correo electrónico individual será intransferible, con acceso exclusivo y personal del servidor correspondiente, además podrán generarse cuentas para uso especial, atendiendo a las necesidades de cada una de las unidades que así lo requieran a la Unidad de Tecnología e Informática.
- g. Cuando se configure la cuenta del servidor, se requerirá que este cambie la clave de acceso por medio del inicio de sesión del sistema operativo Windows vigente, con lo que se brinda mayor seguridad para que solo el titular de la cuenta de correo la conozca y use.
- h. Luego de configurar la cuenta de correo electrónico, se habilitará la opción de "Archivar" el correo histórico, lo que permitirá administrar la información del usuario y evitar que se sature la bandeja de entrada.
- i. Las creaciones y eliminaciones de cuentas de los servidores se realizarán siguiendo los lineamientos de este Reglamento para la creación y eliminación de usuarios, mediante solicitud a la Unidad de Tecnología e Informática por parte de la Unidad de Administración de Talento Humano, con los datos personales como nombres completos, número de cédula y puesto en la Institución.
- j. En caso de olvido o bloqueo de la contraseña, el usuario coordinará la habilitación de la cuenta con la Unidad de Tecnología e Informática.

Art. 53.- Tipos de Cuentas.- Se establecen tres tipos de movimientos de cuentas de usuarios bajo los siguientes parámetros:

- a. Alta de perfil de usuario: cuando el usuario ingresa a la Institución o requiere acceso a un nuevo sistema.

b. Modificación de perfil de usuario: cuando el usuario requiere nuevos permisos de acceso a igual información y/o a nueva información.

- c. Baja de perfil de usuario: cuando el usuario no accede más de manera permanente al sistema o se desvincula del Tribunal Contencioso Electoral.

Art. 54.- Contraseña.- La contraseña tiene por objeto garantizar que únicamente el usuario, de acuerdo a su perfil y funciones, tenga acceso a la información pertinente. Se gestionará según las siguientes reglas:

- a. Las contraseñas deben ser de carácter personal e intransferible, deberán mantenerse y manejarse en secreto por el usuario.
- b. Se prohíbe a los servidores del Tribunal Contencioso Electoral dar a conocer su contraseña a terceras personas, quien así lo hiciere, será legalmente responsable de las actividades que se realicen con su identificación de usuario (ID) y contraseña.
- c. De los cuatro (4) grupos de caracteres (mayúsculas, minúsculas, números y caracteres especiales), la clave al menos deberá contener seis (6) caracteres, y como mínimo tres (números), un (1) carácter especial y tres (3) letras.
- d. En caso de que el usuario sospeche que su contraseña ha sido comprometida deberá solicitar inmediatamente su cambio a la Unidad de Tecnología e Informática.
- e. En caso de olvido o bloqueo de su contraseña, el usuario deberá coordinar el restablecimiento de la cuenta con la Unidad de Tecnología e Informática.
- f. Por regla general las contraseñas deberán ser cambiadas periódicamente cada noventa (90) días, de acuerdo con la importancia y la sensibilidad de la información a la que se tiene acceso.
- g. Los servidores del Tribunal Contencioso Electoral deberán utilizar contraseñas que no resulten obvias, fáciles de adivinar o descubrir, o no sean predecibles para un posible atacante, tales como: nombre o apellidos del usuario, fechas o nombres de personas allegadas, secuencias de números repetidos, entre otros. Para que las contraseñas cumplan con su función de seguridad de la información, deberán tener una longitud mínima de 6 caracteres alfanuméricos (número, letras y/o caracteres especiales combinados).
- h. La contraseña no deberá contener el nombre de la cuenta que use para acceder al computador asignado.
- i. La contraseña no deberá ser la misma utilizada en los tres (3) últimos cambios de contraseñas anteriores.

Art. 55.- Respaldos.- Si el servidor del Tribunal Contencioso Electoral requiere obtener un respaldo de sus correos en un archivo independiente, deberá ser autorizado por el jefe inmediato, esto es también aplicable para casos en que un servidor del Tribunal Contencioso Electoral se

separe de la Institución, para lo cual se coordinará con la Unidad de Tecnología e Informática.

Art. 56.- Tamaño del buzón.- El tamaño estándar es de 2 GB, este podrá ser ampliado por solicitud expresa y tomando en cuenta también el cargo del servidor del Tribunal Contencioso Electoral, fundamentado bajo los siguientes parámetros:

- a. Autoridades, máximo hasta 4 GB.
- b. Directores y Asesores, máximo hasta 3 GB.

Art. 57.- Responsabilidad.- El proceso de respaldo de los buzones de correo electrónico de los servidores del Tribunal Contencioso Electoral tiene un carácter de responsabilidad compartida entre el usuario, quien conoce que ha respaldado o no, y el personal de soporte técnico, que realice la descarga de sus correos personales e institucionales al equipo asignado. En caso de requerir este servicio de respaldo se lo solicitará a la Unidad de Tecnología e Informática.

Art. 58.- Administración de correos asociados.- Los correos de los sistemas asociados que tienen buzones de recepción de la ciudadanía deberán ser administrados por el servidor del Tribunal Contencioso Electoral del área correspondiente y se ejecutará el mismo procedimiento en el equipo asignado para esta labor.

Art. 59.- Revisión y control.- De existir causa justificada por escrito y so pena de sanciones administrativas, civiles y penales de quien lo solicite, las cuentas de correo electrónico serán susceptibles de revisión por parte de Auditoría Interna y de la Unidad de Tecnología e Informática, previo el conocimiento y autorización de su titular en caso de que la relación laboral este vigente.

Art. 60.- Envío de información masiva.- Únicamente los correos institucionales emitidos por la Unidad de Comunicación Social y la Unidad de Tecnología e Informática del Tribunal Contencioso Electoral y aquellos que la Dirección Administrativa Financiera autorice, contendrán comunicados generales mediante el envío masivo por las listas de distribución existentes.

Los envíos de mensajes masivos por correo electrónico solo podrán contener información de interés general y relacionada con las actividades o funciones propias de la Institución.

Queda totalmente prohibida cualquier difusión masiva de anuncios electrónicos de tipo personal.

Art. 61.- Prevención de virus y programas maliciosos.- La Unidad de Tecnología e Informática utilizará programas que monitoreen el accionar de los virus informáticos tanto para los mensajes de correo como para todos los archivos adjuntos previamente a su ejecución, para lo cual:

- a. Instalará y vigilará la actualización del software de antivirus y código malicioso.
- b. Mantendrá los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.

c. Revisará periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Institución.

d. Verificará antes de su uso la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables.

e. Concienciará al personal de la Institución acerca del problema de los virus y como proceder frente a los mismos.

f. Se prohíbe introducir en los computadores personales cualquier tipo de medio de almacenamiento sin que previamente haya sido revisado por el software antivirus de la Institución, para descartar la presencia de virus o cualquier otro programa dañino.

g. Se prohíbe conectar en la red institucional cualquier equipo de computación y/o dispositivo móvil sin la autorización y la revisión previa de la Unidad de Tecnología e Informática.

h. Se prohíbe grabar en los dispositivos de almacenamiento de los equipos de computación personales cualquier tipo de archivo de dudosa condición o calidad que pueda ocasionar daños. Esto aplica a archivos procedentes de Internet o introducidos al PC por medio de dispositivos de almacenamiento externos (ejemplo: disco duro externo, flash memories o de cualquier otra índole) sin que se tenga la certeza de que están libres de códigos maliciosos.

i. El usuario verificará regularmente que su equipo de computación disponga de software antivirus actualizado. De no contar con dicha herramienta o en caso de duda, está obligado a solicitar a la Unidad de Tecnología e Informática su inmediata actualización.

j. El usuario deberá abstenerse de abrir, responder o reenviar mensajes de correo electrónico que no provengan de fuentes conocidas y seguras, y descargar anexos enviados por correo electrónico que puedan ser fuente de virus o similares o cuya procedencia y características desconozca.

k. El usuario en caso de presumir o evidenciar la presencia de virus o similares en su equipo de computación, deberá de inmediato salir de los programas que al momento esté ejecutando, apagar el computador, notificar a la Unidad de Tecnología e Informática a través de correo electrónico, asegurándose que su requerimiento ha sido registrado y atendido eficazmente.

Art. 62.- Notificación de errores.- Todo sistema tendrá implementadas facilidades automáticas que permitan al usuario ser notificado con error con la recepción de un mensaje, en caso de que dicho mensaje no sea recibido correctamente por el destinatario seleccionado, notificación que describirá detalladamente el motivo del error.

Art. 63.- Encriptación y firma electrónica.- Para el uso de información sensible, envío y conservación, se

implementará la facilidad de encriptación de datos y firma electrónica, en la medida que lo permitan los sistemas utilizados.

Capítulo V DISPOSITIVOS PORTÁTILES

Sección I Webmail

Art. 64.- Definición.- Opción tecnológica mediante la cual se puede efectuar una conexión remota al buzón de correo institucional, esta conexión puede ser realizada por medio de cualquier navegador existente siendo recomendable utilizar Mozilla Firefox para asegurar la completa funcionalidad.

Art. 65.- Responsabilidades del usuario.- Son responsabilidades de usuario las siguientes:

- a. Acceder al webmail a través de un computador libre de programas que amenacen la seguridad de la cuenta.
- b. Tomar las precauciones necesarias si utiliza esta funcionalidad desde un computador público.
- c. Asegurar que la sesión sea cerrada al momento de dejar de utilizar esta funcionalidad.

Art. 66.- Responsabilidades de la Unidad de Tecnología e Informática.- Son sus responsabilidades las siguientes:

- a. Mantener la seguridad por medio de una solución de seguridad para garantizar la protección del servidor de correo.
- b. Garantizar la disponibilidad del servicio en un 96% de uptime mensual.

Sección II Dispositivos Móviles

Art. 67.- Definición.- Son herramientas, dispositivos o equipos tecnológicos (tablets, smartphones, computadores portátiles) que permiten a los servidores del Tribunal Contencioso Electoral gestionar su cuenta de correo y agenda electrónica en cualquier lugar; para ello se utilizarán dispositivos portátiles que brinden estas ventajas.

Art. 68.- Responsabilidades del usuario.- Son responsabilidades de usuario las siguientes:

- a. Utilizar redes de comunicación seguras en el caso de existir una conexión mediante WiFi.
- b. El uso del dispositivo institucional móvil debe ser personal y procurar que personas no autorizadas no tengan acceso al mismo.
- c. En caso de pérdida, robo o hurto del dispositivo institucional móvil, informar al personal de sistemas para cambiar la contraseña de la cuenta respectiva.

d. Mantener el dispositivo institucional móvil libre de programas peligrosos que puedan atentar contra la información institucional.

e. Mantener actualizado tecnológicamente el dispositivo institucional móvil.

f. Revisar de forma continua los correos enviados y recibidos desde el dispositivo institucional móvil.

Art. 69.- Responsabilidades de la Unidad de Tecnología e Informática.- Son sus responsabilidades las siguientes:

- a. Mantener garantías orientadas a una óptima seguridad, a través de soluciones precisas e inmediatas a fin de lograr protección del servidor institucional de correo.
- b. Garantizar la disponibilidad del servicio en un 96% de uptime mensual.
- c. Monitorear periódica e indistintamente el uso y manejo de los recursos tecnológicos institucionales a fin de verificar su correcto uso, y en caso de encontrar novedades, notificar inmediatamente lo ocurrido al titular de la Dirección Administrativa Financiera.

Capítulo VI SERVICIO DE INTERNET Sección I Uso del servicio

Art. 70.- Reglas sobre el uso.- Internet es un servicio que el Tribunal Contencioso Electoral pone a disposición de sus servidores públicos, para uso estrictamente laboral. Al hacer uso del Internet el usuario debe seguir las siguientes reglas:

- a. Utilizar el Internet apropiadamente, de acuerdo a lo establecido en este Reglamento.
- b. Verificar que la información que acceda en el Internet sea exacta, completa y actual.
- c. El servicio de Internet debe utilizarse exclusivamente para las tareas propias de la función desempeñada en la Institución y no para ningún otro fin.
- d. La utilización del Internet y servicios anexos será únicamente destinado para consulta y verificación de información en sitios considerados de apoyo al desempeño de actividades propias del cargo que desempeña el servidor del Tribunal Contencioso Electoral.
- e. Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la Institución.
- f. La Unidad de Tecnología e Informática tendrá la obligación de limitar a los usuarios el acceso a portales, aplicaciones o servicios de Internet y la Web que

- podrían perjudicar los intereses, la productividad y la reputación de la Institución. Específicamente, se bloqueará el acceso por medio de dispositivos fijos y/o móviles a todos aquellos sitios no considerados útiles en el desempeño de las funciones del servidor del Tribunal Contencioso Electoral, en base a los perfiles del puesto; y, el acceso a portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses y valores de la Institución o que impacten negativamente en la productividad y trabajo de sus servidores (como mensajería instantánea-chats, redes sociales, video, otros), particularmente a los que atenten a la ética, la moral y buenas costumbres. La Unidad de Comunicación Social es la responsable de administrar las cuentas de redes sociales de la institución, por tal motivo esta dirección tendrá habilitado el acceso a los sitios o portales Web de redes sociales.
- g. Los usuarios no deben utilizar el servicio de Internet mediante los recursos informáticos o de red del Tribunal Contencioso Electoral con fines recreativos o de entretenimiento.
- h. Queda totalmente prohibido el uso de programas como aTube Catcher, Emule, Ares, Kazaa y cualquier otro programa P2P (Peer to Peer).
- i. No se deberá buscar, hacer uso o apoderarse de información personal, ni se deberán obtener copias del software, archivos, datos ni contraseñas pertenecientes a otros usuarios de Internet. No se deberá llevar a cabo en ningún caso la suplantación de forma voluntaria y consciente de otro usuario.
- j. El usuario no debe descargar del internet ningún programa (software) tales como: Shareware, software de valuación, etc., archivos de música (MP3, WAV, MPEG-2, MPEG-4).
- k. El usuario queda prohibido de instalar algún tipo de programa para escuchar MP3, RAR, WAV, o emisoras de radio vía Internet (Winamp, REAL AUDIO, MUSIC MATCH, Oozic PLAYER), sin la autorización de su inmediato superior.
- l. Quedan estrictamente prohibidas las redes de tipo social (Facebook, Hi5, twitter, etc.), sin la autorización de su inmediato superior, autorización que se hará bajo su responsabilidad, siempre y cuando se justifique que este acceso será usado únicamente con fines laborales.
- m. Queda estrictamente prohibido el acceso a sitios de contenido sexual, terrorismo, descarga de piratería, media on-demand (videos, tv, radios, streaming en general, youtube).
- n. El usuario que acceda a un sitio de contenido no apropiado deberá responsabilizarse por cualquier eventual contagio o desperfecto al equipo informático desde el que se accede al sitio Web mediante Internet, ocasionado por la sola visita a este tipo de sitio.
- o. Queda estrictamente prohibido transmitir información confidencial o de contenido político, obsceno, amenazante u hostigante que atente en contra de la seguridad del Estado y esta Institución.
- p. El horario de uso del servicio de Internet es libre y estará disponible las 24 (veinticuatro) horas del día, los 365 días del año en la medida de lo posible, considerando además que se realizarán mantenimientos planificados, o en el caso de suspensión del servicio de Internet por caso fortuito o fuerza mayor. En caso de existir alguna falla en el servicio el usuario deberá reportar el inconveniente a la Unidad de Tecnología e Informática.
- q. La Máxima Autoridad o su delegado autorizará a los servidores del Tribunal Contencioso Electoral el acceso a sitios Web en Internet u otros servicios informáticos, los cuáles no se encuentren permitidos, con la debida justificación del Jefe de la unidad administrativa en la que trabaja el servidor.
- r. El titular de cada unidad podrá requerir acceso a sitios bloqueados de internet indicando los motivos que justifiquen su requerimiento.
- s. El consumo de ancho de banda por usuario será monitoreado y en casos de encontrar un consumo excesivo por varias ocasiones, queda a discreción de la Unidad de Tecnología e Informática solicitar la justificación del mismo al titular de la unidad, de considerarlo conveniente, a fin de analizar y tomar las medidas del caso.
- t. Comprobar (de ser posible) la validez de la información encontrada. En el caso de ser información de otras instituciones, se requerirá que se confirme la información obtenida por internet mediante solicitud escrita o por correo electrónico.
- u. Respetar las protecciones legales de los datos y software proporcionados por sus derechos de autor y licencias.
- v. Informar inmediatamente a la Unidad de Tecnología e Informática sobre cualquier ocurrencia inusual que suceda en el uso de este servicio.
- El jefe de cada Despacho de Juez, Dirección o Unidad reportará el uso inadecuado de Internet o el acceso a páginas no autorizadas a la Unidad de Tecnología e Informática, con la finalidad de que se investigue si efectivamente ha existido mal uso del servicio de Internet, y de ser el caso, se restrinja el acceso a dichas páginas al infractor. El jefe de cada Despacho de Juez, Dirección o Unidad, velará por el cumplimiento de las normas del presente Reglamento por parte del personal a su cargo.
- De igual manera, si la Unidad de Tecnología e Informática detectare el mal uso que se le dé al servicio de Internet por parte de un usuario, informará al jefe de cada Despacho de Juez, Dirección o Unidad sobre el hecho, con la finalidad de que se investigue y de ser el caso se restrinja el acceso a páginas no autorizadas.

El mal uso que se le dé al servicio de Internet, por inobservancia de deberes, prohibiciones y obligaciones, por parte de un usuario de esta Institución, dará lugar a la sanción administrativa correspondiente, que se impondrá respetando en todo momento el debido proceso y el derecho a la legítima defensa.

Art. 71.- Aplicación de las políticas de uso de Internet-La infracción a las obligaciones establecidas en este Reglamento podrán ser sancionadas de conformidad a lo dispuesto en la Ley Orgánica del Servicio Público (LOSEP), respetando en todo momento el debido proceso y el derecho a la legítima defensa.

La Unidad de Tecnología e Informática velará por el cumplimiento de estas políticas, resguardando los intereses de la Institución.

La Unidad de Tecnología e Informática no se hará responsable por incidentes producidos por el incumplimiento del presente Reglamento.

Capítulo VII SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX

Art. 72.- Definición.- El Sistema de Gestión Documental es una herramienta tecnológica, puesta a disposición de todas las entidades públicas, para efectivizar y agilizar el manejo de información y documentación. El sistema de gestión documental Quipux tiene las siguientes características técnicas:

- a. Conservación intacta de los documentos a lo largo del tiempo;
- b. Acceso inmediato a los documentos independientemente del lugar geográfico;
- c. Búsqueda de documentos definiendo criterios de acceso de forma flexible y fácil;
- d. Consulta simultánea de varios lectores, reproducción;
- e. Envío de documentos obviando el traslado físico;
- f. Inviolabilidad de la información a través de mecanismos de seguridad digital;
- g. Minimización de tiempos de distribución y consulta;
- h. Ahorro de recursos físicos y económicos para gestionar los documentos;
- i. Disminución de impresión de documentos; y,
- j. Apoyo a la conservación del ambiente.

Los manuales para el usuario del Sistema de Gestión Documental Quipux podrán consultarse en la ruta <http://www.gestiondocumental.gob.ec>.

Art. 73.- Administración del sistema.- El Presidente del Tribunal Contencioso Electoral o su delegado, designará

al servidor de la Institución que tendrá a su cargo la Administración del Sistema de Gestión Documental Quipux, el cual tendrá acceso al sistema únicamente con los límites establecidos por la Secretaría Nacional de la Administración Pública.

Se garantizará que todos los documentos permanezcan completos, fiables, en cuanto al contenido; auténticos, en cuanto a la originalidad; y accesibles, en cuanto a su localización y legibilidad.

Los documentos digitales tendrán una marca de tiempo que asegure el tiempo exacto de cada operación realizada y la vigencia de la firma electrónica si los mismos hubiesen sido firmados digitalmente.

Art. 74.- Obligaciones de la Unidad de Tecnología e Informática.- Se considerarán como sus obligaciones las siguientes:

- a. Coordinar con la Unidad de Administración de Talento Humano y demás áreas involucradas a fin de identificar y confirmar los servidores del Tribunal Contencioso Electoral a los cuales se les deberá crear un usuario en el Sistema de Gestión Documental Quipux, para el ejercicio de sus funciones.
- b. Definir los perfiles de los servidores del Tribunal Contencioso Electoral que utilicen el Sistema de Gestión Documental Quipux.
- c. Estandarizar las plantillas (institucional/área), que se utilizará para cada documento interno o externo que se genere en el Tribunal Contencioso Electoral.

Art. 75.- Atribuciones del Administrador del Sistema de Gestión Documental- El servidor del Tribunal Contencioso Electoral, que haya sido nombrado como Administrador del Sistema de Gestión Documental Quipux, tendrá las siguientes obligaciones, mismas que ejecutará a través del área tecnológica:

- a. Crear usuarios en el sistema, áreas de la Institución, así como actualizar los cargos y datos de los servidores del Tribunal Contencioso Electoral, de acuerdo a la información remitida por la Unidad de Administración de Talento Humano.
- b. Asignar los perfiles correspondientes a cada servidor del Tribunal Contencioso Electoral en base a la información remitida por la Unidad de Administración de Talento Humano.
- c. Administrar los accesos para el archivo virtual y físico de documentación e información, según lo definido por la Unidad de Administración de Talento Humano.
- d. Administrar el reinicio de claves de los servidores del Tribunal Contencioso Electoral.
- e. Coordinar con la Unidad de Tecnología e Informática la carga de información actual al sistema de gestión documental Quipux.

f. Ejecutar los procedimientos relacionados con la subrogación de cargos, cuya información será suministrada por la Unidad de Administración de Talento Humano.

g. Determinar opciones generales las cuales están asociadas a todos los perfiles, así como también opciones específicas que han sido definidas para cada perfil.

Art. 76.- Accesibilidad y confidencialidad.- Estará delimitada conforme al nivel de acceso que disponga el usuario en el sistema y en los documentos, acceso que depende de la jerarquía, nivel de responsabilidad y permisos. Un documento podrá ser calificado como confidencial para restringir su acceso.

Capítulo VIII SISTEMAS INFORMÁTICOS JURISDICCIONALES

Art. 77.- Definición.- Los sistemas informáticos jurisdiccionales son herramientas tecnológicas bajo plataforma Web puestas a disposición de los servidores para el ingreso, tratamiento y reporte de información jurisdiccional, mediante perfiles de usuario y roles específicos.

Art. 78.- Administración.- El responsable de la Unidad de Tecnología e Informática tendrá a su cargo la administración, control, respaldo y optimización de los servidores de cómputo donde reposan los sistemas informáticos jurisdiccionales habilitados.

El Secretario General del Tribunal Contencioso Electoral conjuntamente con el responsable de la Unidad de Tecnología e Informática, garantizarán el uso, gestión y disposición de la información contenida en los mismos; en tal razón, avalarán que toda la información permanezca completa y fiable; auténtica, en cuanto a la originalidad; y accesibilidad, en cuanto a su localización e integridad.

Los tiempos de conservación o depuración de la información deberá ser establecida por la Máxima Autoridad o su delegado.

Art. 79.- Modificaciones.- Cualquier modificación a los sistemas informáticos jurisdiccionales deberá ser evaluada por la Unidad de Tecnología e Informática desde el punto de vista de viabilidad técnica y luego ser aprobada por la Máxima Autoridad o su delegado, previo informe del Comité de Seguridad de la Información.

Art. 80.- Desarrollos.- Cualquier desarrollo respecto de sistemas informáticos jurisdiccionales deberá ser evaluado por la Unidad de Tecnología e Informática y aprobado por la Máxima Autoridad o su delegado, bajo los siguientes aspectos:

Área requirente

Entrega de flujos de acciones del sistema con sus respectivos datos de entrada, procesamiento y reportes del mismo; y,

entrega del cronograma propuesto donde se contemplen tiempos de desarrollo, implementación, pruebas, optimización y puesta en producción de la herramienta.

Área administrativa-técnica

Disponibilidad de personal, disponibilidad de hardware y viabilidad técnica.

En caso de cumplir los plazos y disponibilidades técnicas planteadas por el área requirente y área administrativa-técnica, se entregará un cronograma de actividades adaptado a los tiempos planteados o consensuados con el área requirente.

Capítulo IX SISTEMAS INFORMÁTICO ADMINISTRATIVOS

Art. 81.- Definición.- Los sistemas informáticos administrativos, son herramientas tecnológicas bajo plataforma Web, puestas a disposición de los servidores que conforman la Institución para el ingreso, tratamiento y reporte de información almacenada, mediante perfiles de usuario y roles específicos.

Art. 82.- Administración.- El responsable de la Unidad de Tecnología e Informática tendrá a su cargo la administración, control, respaldo y optimización de los servidores de cómputo donde reposan los sistemas informáticos administrativos.

El Director Administrativo Financiero y el responsable de la Unidad de Tecnología e Informática, en forma conjunta, garantizarán el uso, gestión y disposición de la información contenida en los sistemas informáticos administrativos; en tal razón, avalarán que toda la información permanezca completa y fiable; auténtica, en cuanto a la originalidad; y accesibilidad, en cuanto a su localización e integridad.

Art. 83.- Modificaciones.- Cualquier modificación a los sistemas informáticos administrativos deberá ser evaluada por la Unidad de Tecnología e Informática desde el punto de vista de viabilidad técnica y luego ser aprobada por el Director Administrativo Financiero, previo informe del Comité de Seguridad de la Información.

Art. 84.- Desarrollos.- Cualquier desarrollo respecto de sistemas informáticos administrativos deberá ser evaluado por la Unidad de Tecnología e Informática en conjunto con el Director Administrativo Financiero, una vez que los mismos hayan sido elaborados por las áreas requirentes, bajo los siguientes aspectos:

Área requirente

Entrega de flujos de acciones del sistema con sus respectivos datos de entrada, procesamiento y reportes del mismo; y, entrega de cronograma propuesto donde se contemplen tiempos de desarrollo, implementación, pruebas, optimización y puesta en producción de la herramienta.

Área administrativa-técnica

Disponibilidad de personal, disponibilidad de hardware y viabilidad técnica.

En caso de cumplir los plazos y disponibilidades técnicas planteadas por el área requirente y área administrativa-técnica, se entregará un cronograma de actividades adaptado a los tiempos planteados o consensuados con el área requirente.

**Capítulo X
CONTROL**

Art. 85.- Claves de acceso.- La Unidad de Tecnología e Informática, conjuntamente con Servicios Generales son responsables de la asignación y la administración de la asignación de claves de acceso a los recursos tecnológicos de la Institución.

Art. 86.- RespalDOS.- La Unidad de Tecnología e Informática estará encargada de generar procesos de respaldo diarios de los buzones para autoridades del Tribunal Contencioso Electoral, siempre y cuando el usuario no los haya descargado a su equipo. Este servicio está configurado con alertas automáticas al alcanzar el umbral del 75% del tamaño de buzón y notificar a los servidores del Tribunal Contencioso Electoral la limpieza de los mismos.

Art. 87.- Responsabilidades.- Los servidores a quienes se autorice la entrega y uso de los bienes, equipos, sistemas informáticos, el correo electrónico institucional, los dispositivos móvil-USB y cualquier otro servicio o sistema, serán responsables de su cuidado, buen uso, destino y conservación, durante el período de tiempo de su gestión o el tiempo que les fuere autorizado su utilización, o la vigencia del respectivo contrato o nombramiento.

Los servidores que hagan uso de los bienes, equipos, sistemas informáticos del correo electrónico institucional, los dispositivos móvil-USB y cualquier otro servicio o sistema, tendrán la obligación de conocer y acatar cualquier instrucción administrativa que se emita sobre el uso y conservación de los mismos, que solo podrán ser utilizados con fines lícitos e inherentes a las actividades oficiales y funciones propias de la Institución, para lo cual informarán oportunamente y por escrito a la Dirección Administrativa Financiera, sobre cualquier novedad que se presente con relación a los mismos o la contravención a las disposiciones contenidas en este instrumento, a fin de adoptar las medidas correctivas que fueren pertinentes para el caso.

De verificarse que algún servidor use los bienes, equipos, sistemas informáticos del correo electrónico institucional, los dispositivos móvil-USB, del servicio de Internet y cualquier otro servicio o sistema provisto por la Institución, para fines ajenos al servicio público o con accesos no autorizados, el custodio o responsable de los mismos deberá justificar dicha situación ante la Dirección Administrativa Financiera, quien a través de la Unidad de Tecnología e Informática levantará un informe donde se determinen los correctivos a tomarse, se establezcan recomendaciones o se determinen responsabilidades o la posible determinación

de sanciones administrativas a quienes hubieren incurrido en estos hechos, previo la presentación de los descargos correspondientes y el cumplimiento del debido proceso a cargo de la Unidad de Administración de Talento Humano.

Art. 88.- Responsabilidad de la Unidad de Tecnología e Informática.- Son sus responsabilidades las siguientes:

- a. Mantener los respaldos de la información procesada y almacenada en los equipos y sistemas durante el tiempo que establezca la normativa legal aplicable.
- b. Entregar a cada usuario las herramientas tecnológicas necesarias para su trabajo.
- c. Realizar control de la utilización de recursos tecnológicos e informar a la Unidad de Administración de Talento Humano sobre el mal uso de los mismos por parte del usuario.
- d. Poner a disposición de los servidores del Tribunal Contencioso Electoral un sistema de soporte técnico con el fin de gestionar la solución de problemas y llevar un control de los mismos para garantizar la integridad, confidencialidad y disponibilidad de la información.
- e. Difundir las regulaciones adoptadas en el presente instrumento, a través de circulares u otros medios que considere conveniente para una efectiva socialización al personal del Tribunal Contencioso Electoral previo a su ejecución.
- f. Monitorear permanentemente los accesos a la red institucional de datos y en caso de ser necesario con la colaboración de expertos informáticos externos.
- g. Las demás responsabilidades establecidas en el presente Reglamento a la Unidad de Tecnología e Informática u otras normas aplicables a los procesos de gestión a su cargo.

**Capítulo XI
PROHIBICIONES**

Art. 89.- Prohibiciones.- Se prohíbe a los servidores del Tribunal Contencioso Electoral lo siguiente:

- a. El uso para actividades particulares de los bienes, equipos, sistemas informáticos, el sistema de correo electrónico institucional y cualquier otro servicio o sistema provisto por la Institución.
- b. El acceso, manejo, intercambio o transmisión de material obsceno u ofensivo, a través de los sistemas informáticos, computacionales o del sistema de comunicación electrónica, el acceso a material erótico, realizar a través de ellos bromas de cualquier forma o cualquier comentario que pueda constituir un acto discriminatorio o de hostigamiento sexual.
- c. El intercambio de archivos con contenidos ajenos a las funciones que desempeñen los servidores del Tribunal Contencioso Electoral.



- d. La navegación virtual por sitios de Internet relacionados con temas tales como sexo, racismo, guerra, violencia, fundamentalismo, diversión, entretenimiento, redes sociales y en general sitios ajenos a las actividades de los servidores del Tribunal Contencioso Electoral.
- e. El uso del correo electrónico con fines de propaganda, manifestaciones u opiniones religiosas, políticas, partidistas o electorales por parte de servidores del Tribunal Contencioso Electoral.
- f. La entrega del listado de contactos de correo electrónico de servidores del Tribunal Contencioso Electoral a terceros sin el permiso de la autoridad competente, previa justificación correspondiente.
- g. La distribución masiva de grandes cantidades de mensajes sean o no de contenido institucional a direcciones externas o dentro de la misma Institución.
- h. El uso de redes sociales, programas de charlas o similares sin la debida autorización de la Unidad de Comunicación Social.
- i. Utilizar o destinar los bienes, equipos, sistemas informáticos, correo institucional, el servicio de Internet inalámbrico y demás bienes o servicios en actos que atenten contra la seguridad del Estado, el orden público, la moral y las buenas costumbres o para realizar actos que desprestigien y afecten a la imagen de la Institución, de sus autoridades y compañeros o para actividades de proselitismo político, comercial o religiosas.
- j. Usar las computadoras, equipos informáticos, internet y sistema de mensajería institucional para propósitos personales, de ocio, para manejo de un negocio o asuntos privados del usuario; para la recepción y envío de mensajes en cadena, para acceder a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro asunto o servicio ajeno a las labores y funciones propias de la Institución.
- k. Copiar, transferir o utilizar en computadoras personales o que no sean de la Institución, programas (software) adquiridos por esta.
- l. Instalar en las computadoras o equipos informáticos programas que no hayan sido adquiridos por la Institución, sin el conocimiento y autorización previa de la Unidad de Tecnología e Informática.
- m. Acceder, utilizar o disponer de información sujeta a propiedad intelectual (copyrighted information) que viole derechos de autor y aquella que sea confidencial o tenga el carácter reservado, sin la debida autorización.
- n. Acceder, utilizar, disponer, alterar o eliminar información de carácter institucional, sin la debida autorización.
- o. Utilizar el Internet inalámbrico a través del módem, USB o similares, para asuntos particulares o que no

se relacionen con el trabajo, actividades, funciones o responsabilidades que tienen los funcionarios de la Institución en el ejercicio del cargo asignado.

- p. Egresar o sacar de las oficinas o instalaciones equipos informáticos de propiedad de la Institución, sin la debida autorización de la Dirección Administrativa Financiera.

Capítulo XII DISPOSICIONES GENERALES

Primera.- La inobservancia de las normas del presente Reglamento será sancionada de conformidad con el régimen disciplinario de Ley Orgánica del Servicio Público, Reglamento General a la Ley Orgánica del Servicio Público, normativa Institucional vigente referente a la materia sin perjuicio de la responsabilidad que pudiere determinarse conforme la Ley Orgánica de la Contraloría General del Estado y otras leyes vigentes.

Segunda.- La Unidad de Tecnología e Informática se encargará de que en cada monitor asignado a servidores o terceros que presten sus servicios para esta Institución, conste de forma obligatoria el logo institucional del Tribunal Contencioso Electoral como protector de pantalla.

En caso de inobservancia a lo dispuesto, o si a sabiendas de lo señalado, servidores del Tribunal Contencioso Electoral o terceros que presten sus servicios para esta Institución, intenten cambiar el protector de pantalla eliminando el logo institucional, la Unidad de Tecnología e Informática notificará al titular de la Dirección Administrativa Financiera a fin de que se proceda con las medidas correctivas pertinentes.

Tercera.- De la sociabilización y ejecución del presente Reglamento, encárguese a la Unidad de Tecnología e Informática.

Cuarta.- Las disposiciones del presente Reglamento son de carácter especial y prevalecerán sobre otras normas de igual o menor jerarquía que se opongan, a excepción de aquellas específicas de la gestión jurisdiccional del Tribunal Contencioso Electoral que no se contemplan expresamente en este instrumento.

Las políticas y procedimientos de archivo para la conservación y mantenimiento de archivos físicos y magnéticos y el instructivo sobre el uso de celulares del Tribunal Contencioso Electoral, expedidos por la Máxima Autoridad, se aplicarán sin oposición a las normas del presente Reglamento.

Quinta.- El presente instrumento entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Sexta.- Encárguese del cumplimiento y de su ejecución a la Dirección Administrativa Financiera y más unidades del Tribunal Contencioso Electoral.

Registro Oficial - Edición Especial N° 84 Miércoles 13 de septiembre de 2017 - 23

Dado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los veintinueve días del mes de agosto de dos mil diecisiete.

RAZÓN: Siento por tal que la Resolución que antecede fue aprobada por el Pleno del Tribunal Contencioso Electoral en sesión ordinaria de martes 29 de agosto de 2017.

f.) Ab. Ivonne Coloma Peralta, Secretaria General, Tribunal Contencioso Electoral.

RAZÓN.- En mi calidad de Secretaria General del Tribunal Contencioso Electoral CERTIFICO que el ejemplar que antecede, es fiel copia del original que reposa en la Secretaría General del Tribunal Contencioso Electoral y que fue aprobada en sesión ordinaria de martes 29 de agosto de 2017, por el Pleno de este Tribunal.- Lo certifico.-

f.) Ab. Ivonne Coloma Peralta, Secretaria General, Tribunal Contencioso Electoral.

Imagen

Imagen



SECRETARÍA GENERAL



Notificación No. TCE-SG-2017-0025-N

PARA: Dr. Luis Buenaño Orozco
DIRECTOR ADMINISTRATIVO FINANCIERO

Dra. María Paredes Arellano
DIRECTORA DE ASESORÍA JURÍDICA

Dra. Natalia Cantos Romoleroux
DIRECTORA DE INVESTIGACIÓN CONTENCIOSO ELECTORAL

Eco. Medardo Robayo Robayo
DIRECTOR DE AUDITORIA INTERNA

Ing. Ma. Eugenia Velasco Mantilla
UNIDAD DE PLANIFICACIÓN

UNIDAD DE COMUNICACIÓN

DE: Ab. Ivonne Coloma Peralta
SECRETARIA GENERAL

FECHA: 30 de agosto de 2017

Para su conocimiento y fines legales pertinentes comunico a usted (es), que el Pleno del Tribunal Contencioso Electoral, en uso de sus atribuciones constitucionales y legales, en sesión ordinaria de martes 29 de agosto de 2017, a las 10:15, adoptó la siguiente resolución:

"EL PLENO DEL TRIBUNAL CONTENCIOSO ELECTORAL

CONSIDERANDO

- Que,** el numeral 2 del artículo 16 de la Constitución de la República del Ecuador establece como derecho de las personas, en forma individual o colectiva, el acceso universal a las tecnologías de información y comunicación;
- Que,** el numeral 21 del artículo 66 de la Constitución de la República del Ecuador reconoce y garantiza a las personas el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; derecho que protege cualquier otro tipo o forma de comunicación;
- Que,** el artículo 217 de la Constitución de la República del Ecuador crea el Tribunal Contencioso Electoral, con jurisdicción nacional, personalidad jurídica propia y autonomía administrativa, financiera y organizativa;
- Que,** el numeral 3 del artículo 221 de la Constitución de la República faculta al Tribunal Contencioso Electoral para determinar su organización, formular y ejecutar su presupuesto;
- Que,** el artículo 227 de la Constitución de la República establece que la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación;
- Que,** el artículo 233 de la Constitución de la República del Ecuador señala que ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus



SECRETARÍA GENERAL



funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos;

- Que,** los numerales 10 y 11 del artículo 70 de la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia, facultan al Tribunal Contencioso Electoral para expedir la reglamentación necesaria para su funcionamiento, así como, determinar su organización, formular y ejecutar su presupuesto ordinario y el extraordinario para procesos electorales;
- Que,** el artículo 77 de la Ley Orgánica de la Contraloría General del Estado establece la obligación del Titular de la entidad de dirigir y asegurar la implantación, funcionamiento y actualización de los sistemas administrativos;
- Que,** el artículo 41 de la Ley Orgánica del Servicio Público, señala que la servidora o servidor público que incumpliére sus obligaciones o contraviere las disposiciones de esa Ley, sus Reglamentos, así como las leyes y normativa conexa, incurrirá en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiere originar el mismo hecho;
- Que,** la Ley Orgánica de la Contraloría General del Estado, artículo 40, preceptúa que las autoridades, dignatarios, funcionarios y demás servidores de las instituciones del Estado, actuarán con la diligencia y empeño que emplean generalmente en la administración de sus propios negocios y actividades, caso contrario responderán, por sus acciones u omisiones, de conformidad con lo previsto en esa ley;
- Que,** el artículo 2 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos reconoce y otorga igual valor jurídico a los mensajes de datos que a los documentos físicos;
- Que,** el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, artículo 148 y Disposición Transitoria Décima Tercera, determina a las entidades contratantes del sector público orden de prelación en la contratación pública relacionada a software y un plan de migración a software libre;
- Que,** el Reglamento General para la administración, utilización, manejo y control de los bienes y existencias del sector público, considera, en su artículo 4, la reglamentación interna para la administración, uso, control y destino de los bienes del Estado; y en los artículos 103 y 104, disposiciones para el registro y mantenimiento de equipos informáticos, hardware y software;
- Que,** las Normas de Control Interno de la Contraloría General del Estado, Grupo 410 Tecnologías de la Información y Grupo 500 Información y Comunicación, regulan la información y la comunicación y su soporte tecnológico informático, con necesaria referencia a un modelo de información de la organización que facilite la creación, uso y compartición de la misma y garantice su disponibilidad, integridad, exactitud y seguridad, sobre la base de la definición e implantación de los procesos y procedimientos correspondientes;
- Que,** la Norma de Control Interno 410-04 Políticas y procedimientos, determina a la Unidad de Tecnología de Información definir, documentar y difundir políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, considerándose temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información; así mismo, la incorporación de controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos; y, la implantación de procedimientos de supervisión de las funciones de tecnología de información;
- Que,** la Norma de Control Interno de la Contraloría General del Estado 410-14 Sitio web, servicios de



internet e intranet, asigna a la Unidad de Tecnología de Información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos;

- Que,** la Norma de Control Interno 300-03 Valoración de los riesgos, determina “Se consideran factores de alto riesgo potencial los programas o actividades complejas... sistemas de información rediseñados... nueva tecnología, entre otros. La valoración del riesgo se realiza usando el juicio profesional y la experiencia”;
- Que,** el artículo 19 del instructivo para el control de bienes del Tribunal Contencioso Electoral, dispone a la Unidad de Tecnología e Informática el plan anual de mantenimiento de los bienes tecnológicos, financiado con el pertinente presupuesto;
- Que,** los estándares del esquema gubernamental de seguridad de la información EGSI, emitido por la Secretaría Nacional de la Administración Pública, son en sentido técnico aplicables en los procesos de gestión del Tribunal Contencioso Electoral;
- Que,** se cuenta con las normativas expedidas en la materia por instituciones del sector público, con sujeción al marco legal aplicable, para sustentar políticas administrativas de gestión tecnológica e informática pertinentes en el Tribunal Contencioso Electoral;
- Que,** mediante Resolución de Pleno No. PLE-TCE-392-23-06-2015, publicada en el Registro Oficial Suplemento 552 de 27 de julio de 2015, se expide el Estatuto Orgánico de Gestión Organizacional por Procesos del Tribunal Contencioso Electoral;
- Que,** el Estatuto Orgánico de Gestión Organizacional por Procesos del Tribunal Contencioso Electoral, señala las atribuciones, responsabilidades y productos de la Unidad de Tecnología e Informática; y,
- Que,** es necesario establecer disposiciones internas para asegurar a los servidores del Tribunal Contencioso Electoral el acceso a la información y la comunicación, para el desarrollo de sus tareas y actividades habituales, a la par que garantizar el uso adecuado, transparente y efectivo de los recursos públicos asignados.

En ejercicio de sus atribuciones constitucionales y legales.

RESUELVE

Expedir el siguiente,

REGLAMENTO DE GESTIÓN TECNOLÓGICA E INFORMÁTICA PARA EL TRIBUNAL CONTENCIOSO ELECTORAL

Capítulo I

DISPOSICIONES PRELIMINARES

Sección I

Objeto, ámbito, principios y obligatoriedad

Art. 1.- Objeto.- El presente instrumento tiene por objeto reglamentar la administración, uso y acceso de los recursos tecnológicos e informáticos del Tribunal Contencioso Electoral, mediante políticas y estándares correspondientes, a fin de alcanzar los objetivos institucionales en el contexto de autenticidad, confiabilidad, confidencialidad, integridad, auditabilidad, protección a la duplicación, no repudio, seguridad, disponibilidad y legalidad de la información que se produce, procesa, intercambia, reproduce y conserva en los procesos organizacionales.



Art. 2.- Ámbito.- Se sujetarán a la presente reglamentación los bienes de la infraestructura tecnológica; los servicios de red como son telefonía fija y móvil, internet, página web, correo electrónico, consultas de información legal; el sistema de gestión documental y las aplicaciones informáticas administrativas y jurisdiccionales desarrolladas y/o adquiridas; y, otras facilidades de base tecnológica informática con acceso habilitado a las y los servidores públicos del Tribunal Contencioso Electoral y/o terceros que interactúan con la Institución.

Art. 3.- Principios.- Las normas del presente instrumento se aplicarán bajo los principios de eficiencia, eficacia, calidad, buenas prácticas y responsabilidad.

Art. 4.- Obligatoriedad.- El cumplimiento del presente instrumento es obligatorio para todos los servidores del Tribunal Contencioso Electoral; así como también para terceros con quienes interactúan de manera habitual u ocasional y que además acceden a información sensible y/o a los recursos tecnológicos e informáticos de la Institución.

Las normas del presente Reglamento referidas a servidores del Tribunal Contencioso Electoral obligan en lo que corresponda a los demás usuarios. En caso de inobservancia se establecerá la responsabilidad a que hubiere lugar.

Sección II Política institucional

Art. 5.- Directrices.- La gestión tecnológica e informática, en orden al cumplimiento de la misión, visión y objetivos estratégicos y operativos institucionales y, con la finalidad de garantizar la seguridad de la información del Tribunal Contencioso Electoral en los medios y el tiempo que su legitimidad y mérito requiera, se orientará por las directrices administrativas que se detallan a continuación; definiéndose y ejecutándose en conformidad los procesos, procedimientos y tecnologías en la medida en que generan, registran, utilizan, procesan, comparten, reproducen, recuperan, conservan y archivan información pública e información pública confidencial o reservada, en medio electrónico o escrito:

- a. La seguridad de la información preservará las características de autenticidad, confiabilidad, confidencialidad, integridad, auditabilidad, protección a la duplicación, no repudio, disponibilidad y legalidad de la información, verificadas previo análisis de riesgos y control de calidad.
- b. La gestión organizacional por procesos incorporará las tecnologías de la información y comunicación con la finalidad de asegurar la calidad, control, productividad, transparencia y continuidad del servicio público de justicia contencioso electoral; y, lo propio en los correspondientes procesos gobernantes, habilitantes, operativos y de seguimiento.
- c. Las tecnologías de la información y comunicación aplicadas cumplirán los estándares de seguridad de la información contemplados en el Esquema Gubernamental de Seguridad de la Información EGSI, en los términos establecidos por la normativa institucional interna del Tribunal Contencioso Electoral.
- d. La planificación estratégica efectuará las previsiones necesarias y la programación presupuestaria consultará el financiamiento del desarrollo de la infraestructura tecnológica e informática que soporta el modelo de información organizacional estructurado.
- e. El sistema de gestión documental administrativo, sobre la base del principio de coordinación del sector público, propenderá a la homologación con el sistema operativo en la Función Ejecutiva y la implementación del uso de la firma electrónica.
- f. El modelo de información de la organización reflejará una política de datos abiertos, salvo excepciones contempladas en norma legal competente, en especial las pertinentes a la gestión jurisdiccional respecto de reserva de la información conforme la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia, y la información pública clasificada confidencial a los efectos de la Ley Orgánica de Transparencia y Acceso a la Información Pública.
- g. La gestión tecnológica e informática en el Tribunal Contencioso Electoral se ajustará rigurosamente a la base legal de sus correspondientes procesos organizacionales, conforme los principios de legalidad, jerarquía normativa y competencia; y, en especial, a las normas pertinentes y aplicables



de control interno emitidas por la Contraloría General del Estado, Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, su Reglamento General, Reglamento para la adquisición de software por parte de las entidades contratantes del sector público, Resoluciones del SERCOP, los principios de vigencia, transferencia y desagregación tecnológica, el Estatuto Orgánico de Gestión Organizacional por Procesos del Tribunal Contencioso Electoral, el presente Reglamento y más normativa aplicable en las instituciones del sector público.

Sección III

Glosario de Términos

Art. 6.- Definiciones.- Para efectos de la aplicación de la presente reglamentación, se considerarán las siguientes definiciones:

- 1. Active Sync:** Es un programa de sincronización de datos desarrollado por Microsoft para su uso con sus sistemas operativos Microsoft Windows, proporciona a los usuarios de Microsoft Windows, una manera de transportar los documentos, calendarios, listas de contacto y correo electrónico entre la computadora de escritorio y un dispositivo móvil, como un PC de mano, teléfonos móviles, o cualquier otro dispositivo portátil que soporte el protocolo de ActiveSync. El protocolo usado para esto es Exchange ActiveSync.
- 2. Administración de riesgos:** Comprende el proceso de control y minimización, o la completa eliminación, de los riesgos de seguridad que podrían afectar a la información de la Institución.
- 3. Auditabilidad:** Asegura que todos los eventos de un sistema deben quedar registrados, permitiendo así su control posterior, ya sea en forma automática o manual.
- 4. Autenticidad:** Propiedad que asegura el origen de la información y la identidad del emisor, misma que puede ser validada, de modo que se demuestre que es quien dice ser; en consecuencia, asegura la validez de la información en tiempo, forma y distribución; y, asimismo, garantiza el origen de la información al validar el emisor de ésta, para evitar suplantación de identidades.
- 5. Confiabilidad:** La información debe ser adecuada para sustentar la toma de decisiones y la ejecución de las actividades propias de la Institución.
- 6. Confidencialidad:** Es la propiedad de la información, por la que se garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma. La confidencialidad se entiende en el ámbito de la seguridad informática, como la protección de datos y de la información intercambiada entre un emisor y uno o más destinatarios frente a terceros.
- 7. Correo electrónico:** Servicio de transmisión de mensajes a través de una red, los cuales pueden incluir archivos adjuntos.
- 8. Corresponsabilidad:** Es la responsabilidad compartida entre dos o más sujetos, es decir que dicha responsabilidad es común entre quienes comparten una obligación o compromiso respecto de algo o de algún evento específico.
- 9. Unidad de Tecnología e Informática:** Encargada de administrar y gestionar las tecnologías de información y comunicación dentro del Tribunal Contencioso Electoral.
- 10. Disponibilidad:** Prevenir interrupciones no autorizadas/controladas de la dotación de recursos y servicios tecnológicos e informáticos. Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, siempre que lo requieran.
- 11. Equipo informático:** Se refiere a todas las partes tangibles o físicas de un sistema informático.
- 12. Esquema Gubernamental de la Información, EGSi:** Instrumento acordado por la Secretaría Nacional de la Administración Pública [Registro Oficial Suplemento 88 de 25 de septiembre de 2013].
- 13. Evaluación de riesgos:** Comprende las acciones realizadas para identificar y analizar las amenazas y vulnerabilidades relativas a la información y a los medios de procesamiento de la misma, así como la probabilidad de ocurrencia y el potencial impacto a las operaciones de la Institución.
- 14. GB o Gigabyte:** Es la unidad de medida de cantidad de datos informáticos. Es un múltiplo del megabyte (MB), que equivale a 1024 MB.
- 15. Hardware:** Se refiere a todas las partes tangibles de un sistema informático; sus componentes pueden ser eléctricos y electrónicos.
- 16. IMAP:** Es un protocolo de aplicación de acceso a mensajes electrónicos almacenados en un servidor, mediante el cual se puede acceder al correo electrónico desde cualquier ordenador que posea una



conexión a Internet, en su estricto nombre es el protocolo de acceso a los mensajes de internet (Internet Message Access Protocol).

17. Incidente de seguridad informática: Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizado de información; un impedimento en la operación normal de las redes de datos, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la política de seguridad de la información de la Institución.

18. Información: Se refiere a toda representación de conocimiento en forma de datos vinculados entre sí, generada utilizando letras, números, gráficos, cartografía, narrativa o audiovisuales; almacenada en cualquier medio, ya sea magnético, papel, pantallas de dispositivos electrónicos u otros.

19. Infraestructura tecnológica: Es el conjunto de hardware y software sobre el que residen los diferentes servicios que requieren estar en funcionamiento para dar soporte tecnológico en el desarrollo de las actividades de la Institución.

20. Integridad: La integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria; por consiguiente, salvaguarda la exactitud y la totalidad de la información y los métodos para su creación, recuperación y procesamiento.

21. Internet: Es una red mundial con millones de usuarios conectados o interconectados entre sí. Estos pueden intercambiar información y establecer distintos servicios tales como: visitar páginas de portales Web, correos electrónicos, charlar o chatear por medio del teclado en los salones creados para este servicio, entre otros.

22. Internet móvil inalámbrico: Es el servicio de acceso inalámbrico a la red internet mediante un modem USB que provee un ISP (Internet Service Provider) o a través de un equipo.

23. Intranet: Red local a la que se accede desde varias localizaciones geográficas distintas y que usa los mismos protocolos de comunicación que internet.

24. Legalidad: Garantizar el cumplimiento de las leyes, normas, Reglamentos o disposiciones.

25. Lista de distribución: Son listas de uso especial del correo electrónico que permite la distribución masiva de información entre múltiples servidores del Tribunal Contencioso Electoral mediante Internet a la misma vez.

26. Mantenimiento correctivo: Aquel que corrige los defectos observados en los equipamientos o instalaciones, es la forma más básica de mantenimiento y consiste en localizar averías o defectos y corregirlos o repararlos.

27. Mantenimiento preventivo: Es el destinado a la conservación de equipos o instalaciones mediante realización de revisión, mantenimiento y reparación periódica que garanticen su buen funcionamiento y fiabilidad. El mantenimiento preventivo se realiza en equipos en condiciones de funcionamiento.

28. MB o Megabyte: Es una unidad de medida de cantidad de datos informáticos. Es un múltiplo del byte u octeto, que equivale a 1000 bytes.

29. Modem USB: Es un dispositivo electrónico que se conecta en un computador para tener acceso al servicio de internet móvil inalámbrico.

30. No repudio: Característica de la información que asegura evitar que una entidad (persona o sistema informático) que haya interactuado con alguna información alegue ante terceros que no lo ha hecho.

31. Perfil de Riesgos Tecnológicos: Es la identificación, cuantificación, control y solución de las posibles amenazas que originan daños en los sistemas.

32. Periféricos: Equipos electrónicos tales como terminales, impresoras, dispositivos auxiliares de computadoras, entre otros.

33. Propietarios de la información: Son los responsables 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.

34. Protección a la duplicación: Característica de la información que asegura que una transacción sea realizada por una única vez, a menos que se especifique lo contrario.

35. Recurso Tecnológico: Es un medio que se vale de la tecnología para cumplir con su propósito.

36. Recurso Informático: Es cualquier componente físico o lógico de disponibilidad limitada en una computadora o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

37. Respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.



- 38. Responsabilidad:** Desarrollar sus funciones a cabalidad y en forma integral dentro de los plazos establecidos por sus superiores y por la ley.
- 39. Seguridad de la información:** Preservación de las siguientes características de la información: confidencialidad, integridad, disponibilidad, autenticidad, auditabilidad, protección a la duplicación, no repudio, legalidad y confiabilidad.
- 40. Seguridades físicas:** Es la precaución que debe tener el usuario del manejo, uso y cuidado de los equipos tecnológicos e informáticos.
- 41. Seguridades lógicas:** Son las contraseñas de usuario, la prevención de contaminación por virus y otros programas que puedan causar daño en los equipos, en la información y otras facilidades.
- 42. Servidores:** Personas que prestan sus servicios al Tribunal Contencioso Electoral y que en razón de sus funciones mantengan en su poder bienes, servicios y aplicaciones de carácter tecnológico de dotación oficial.
- 43. SIP:** Tecnología IP, reemplazo de la telefónica convencional.
- 44. Sistema:** Es el conjunto de partes interrelacionadas, hardware, software y de recurso humano que permite almacenar y procesar información.
- 45. Sistema de Gestión de Seguridad de la Información:** Es un conjunto de políticas de administración de la información, que requiere del diseño, implementación y mantenimiento de un conjunto de procesos y procedimientos que permitan la gestión eficiente de la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de ésta, minimizando los riesgos. Un Sistema de Gestión de Seguridad de la Información debe ser eficiente a través del tiempo, adaptándose a los cambios de la Institución así como a los de su entorno.
- 46. Sistema de Información:** Se refiere a un conjunto de recursos organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información que cumplen con determinadas características propias de la Institución, así como con procedimientos que pueden ser automatizados, manuales o mixtos.
- 47. SMTP:** Es un protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos, en su estricto nombre es el protocolo simple de transferencia de correo (Simple Mail Transfer Protocol).
- 48. Software:** El equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.
- 49. Software libre:** Es la denominación del software que respeta la libertad de todos los usuarios que adquirieron el producto y, por tanto, una vez obtenido el mismo puede ser usado, copiado, estudiado, modificado y redistribuido libremente de varias formas, dependiendo del tipo de licenciamiento libre.
- 50. Software propietario:** Este concepto se aplica a cualquier programa informático que no es libre o que sólo lo es parcialmente (semilibre), sea porque su uso, redistribución o modificación está prohibida, o sea porque requiere permiso expreso del titular del software.
- 51. Spam:** Correo basura considerado no deseado.
- 52. Tecnologías de la información y comunicación:** Se refiere a equipos de cómputo, aplicativos con desarrollo propio o adquiridos, medios de almacenamiento y comunicaciones, que en conjunto son operados por servidores del Tribunal Contencioso Electoral, o por un tercero, con el objetivo de procesar, almacenar y/o transmitir información para llevar a cabo una función propia de la Institución.
- 53. Terceros:** Es toda persona ajena al vínculo jurídico existente entre el servidor o servidora del Tribunal Contencioso Electoral sin distinción del régimen laboral al que pertenezca el cual interactúa de manera habitual u ocasional con el servidor o servidora del Tribunal Contencioso Electoral o con la misma Institución; y, que además acceda a información sensible y/o a los recursos informáticos de la Institución.
- 54. TICs:** Tecnologías de Información y Comunicaciones.
- 55. Uptime mensual:** Es el tiempo que un determinado servicio está disponible en relación al tiempo de medición, en este caso un mes y vinculado estrictamente con un acuerdo de servicio.
- 56. Usuario:** Es el servidor o un tercero que prestan servicios al Tribunal Contencioso Electoral y que utilizan las herramientas informáticas o tecnológicas asignadas a fin de ejecutar sus funciones en la Institución.
- 57. Vulnerabilidades:** Debilidades de las tecnologías informáticas que pueden ser explotadas por una o más amenazas.
- 58. Webmail:** Es un servicio que permite listar, desplegar y borrar vía un navegador web los correos almacenados en un servidor remoto, utilizando un protocolo de correo como IMAP o POP3.



59. WiFi: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica, lleva ese nombre de la sigla de la marca que la creó para referirse a una tecnología de redes inalámbricas. En el estricto nombre (WirelessFidelity) que literalmente significa fidelidad inalámbrica, es en sí un conjunto de estándares y/o protocolos para redes que no requieren de cables y que funcionan en ciertos protocolos previamente establecidos.

60. Zimbra: Es un software libre, que incluye un servidor de correo electrónico.

Sección IV

Propiedad y uso

Art. 7.- Régimen.- La infraestructura tecnológica asignada al servicio público de justicia contencioso electoral es de propiedad del Tribunal Contencioso Electoral.

La propiedad de la información pertinente a la gestión administrativa se verificará sin perjuicio del derecho de acceso a la información pública contemplado en la Ley Orgánica de Transparencia y Acceso a la Información Pública y con observancia de los derechos de propiedad intelectual regulados por el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.

Los equipos, sistemas, aplicaciones, servicios y en general recursos tecnológicos e informáticos solo podrán y deberán ser utilizados con fines lícitos y propios de las competencias del Tribunal Contencioso Electoral.

Sección V

Comité de seguridad de la información

Art. 8.- Comité de Seguridad de la Información.- Con objeto de consulta, definición, informe y supervigilancia de políticas, normas y procedimientos relacionados con la seguridad de la información, su implantación y cumplimiento, se conformará el Comité de Seguridad de la Información del Tribunal Contencioso Electoral integrado por el Presidente del Tribunal o su Delegado, el Director Administrativo Financiero y el responsable de la Unidad de Tecnología e Informática, a fin de cumplir las siguientes responsabilidades:

- a. Proponer: reformas al presente Reglamento, normas complementarias o solicitará a la Máxima Autoridad la aprobación de instructivos, guías u otros instrumentos relacionados con la seguridad de la información en el Tribunal Contencioso Electoral.
- b. Definir e informar la política y normas institucionales en materia de seguridad de la información, gestionar su aprobación por parte del órgano competente y supervigilar el cumplimiento por parte de los servidores de la Institución.
- c. Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes y evaluar los incidentes relativos a la seguridad de la información.
- d. Conocer y recomendar iniciativas para incrementar la seguridad de la información.
- e. Consultar e informar metodologías y procesos específicos relativos a la seguridad de la información y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- f. Promover la difusión y apoyo a la seguridad de la información dentro de la Institución.
- g. Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la Institución frente a incidentes de seguridad imprevistos.
- h. Velar por la provisión de recursos económicos, tecnológicos y humanos necesarios para la gestión de la seguridad de la información.
- i. Solicitar la aprobación de actos administrativos y normativos conducentes a los órganos competentes del Tribunal Contencioso Electoral.

Integrará además el Comité de Seguridad de la Información el Director de Auditoría Interna, con voz pero sin voto con fines de asesoría.

El Comité, convocado por el Administrativo Financiero o su delegado, establecerá la normativa para su



funcionamiento.

Art. 9.- Unidad de Tecnología e Informática.- El responsable de la Unidad de Tecnología e Informática será responsable de la seguridad de la información en la Institución, con las siguientes atribuciones y responsabilidades que cumplirá en forma concordante con las asignadas en el Estatuto Orgánico de Gestión Organizacional por Procesos, las Normas de Control Interno de la Contraloría General del Estado y demás normativa pertinente:

- a. Asegurar la aplicación de los estándares de seguridad de la información establecidos en el presente Reglamento, plan informático estratégico de tecnología, plan de contingencia tecnológica, modelo de información organizacional y más productos/servicios de la Unidad de Tecnología e Informática, con enfoque de gestión de la calidad y administración de riesgos.
- b. Verificar y vigilar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.
- c. Monitorear las necesidades de capacidad tecnológica de los sistemas en operación y proyectar las futuras demandas de esta capacidad para soportar potenciales amenazas a la seguridad de la información que procesan.
- d. Solicitar la reunión del Comité de Seguridad de la Información, cuando la situación lo amerite, actuar en calidad de Secretario, llevar registros de asistencia y actas de las reuniones.
- e. Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones y verificar su cumplimiento; de manera que, no afecten la seguridad de la información.
- f. Informar criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de pruebas antes de su aprobación definitiva.
- g. Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas, equipamiento y verificar su correcta implementación, asignando responsabilidades.
- h. Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones y adoptar o solicitar medidas correctivas.
- i. Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a través de las redes de comunicación de la Institución.
- j. Implementar los controles de seguridad definidos.
- k. Gestionar los incidentes de seguridad de la información de acuerdo al procedimiento aprobado por el Comité de Seguridad de la Información.
- l. Controlar los mecanismos y canales de distribución y difusión de información dentro y fuera de la Institución.
- m. Registrar la documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
- n. Administrar los medios técnicos necesarios para permitir la segregación o separación sistemática de los ambientes de procesamiento.
- o. Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento e informes impresos y verificar la eliminación o destrucción segura de los mismos, cuando proceda.
- p. Administrar y controlar la obtención de copias de resguardo de información, así como la prueba periódica de su restauración.
- q. Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
- r. Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios en los mismos.
- s. Coordinar la gestión de eventos de seguridad con otras entidades gubernamentales.
- t. Coordinar las actividades conducentes, asignar responsabilidades por escrito al personal de la Unidad de Tecnología e Informática y solicitar a los órganos competentes de la Institución los actos o autorizaciones necesarios.

2



- u. Otras atribuciones y responsabilidades establecidas en el presente Reglamento y las que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas y no se encuentren asignadas a un superior jerárquico.

Capítulo II

ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS

Sección I

Asignación, control y mantenimiento de los recursos informáticos

Art. 10.- Asignación por entrega.- Las entregas, revisiones y/o cambios de los equipos, sistemas y recursos informáticos serán requeridas a la Dirección Administrativa Financiera, quien dispondrá a la Unidad de Tecnología e Informática para que, a través de un técnico de su área, proceda con lo solicitado y comunique al titular de la Unidad de Servicios Institucionales para que elabore la respectiva acta de entrega recepción.

La entrega de los equipos o sistemas informáticos la realizará la Dirección Administrativa Financiera con la colaboración de un técnico de la Unidad de Tecnología e Informática, previa suscripción de la respectiva acta de entrega recepción, a la que se acompañará una copia del manual de uso del bien, equipo o sistema para su correcta utilización, cuando el caso lo amerite.

Art. 11.- Custodia.- Los servidores a quienes se autorice la entrega-recepción de los bienes, equipos y sistemas informáticos, serán responsables de su uso, custodia y buena conservación de conformidad a las normas del Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, el presente Reglamento y la normativa institucional.

Cualquier novedad que se presentare con relación a los bienes, equipos o sistemas, será inmediatamente notificada por el custodio a la Unidad de Tecnología e Informática, sin perjuicio del cumplimiento de los procedimientos establecidos en otras normas aplicables.

Art. 12.- Registro y control.- La Dirección Administrativa Financiera será responsable del registro, custodia y administración de los bienes y equipos informáticos; la Unidad de Tecnología e Informática será responsable del control y monitoreo del buen uso, para lo cual:

- Identificará y verificará periódicamente todos los bienes tecnológicos y de comunicaciones en un registro del que constará el historial, estado actual, inventario físico y lógico, coordinará una conciliación con los registros contables financieros, registrará a los custodios y mantendrá un respaldo de las actas de entrega recepción.
- Comprobará el correcto funcionamiento de los bienes, equipos y sistemas informáticos de la Institución.
- Comunicará a la Dirección Administrativa Financiera o a quien corresponda cualquier novedad que se presente respecto a los bienes, equipos y sistemas informáticos de la Institución.
- Cumplirá las atribuciones y responsabilidades que el presente Reglamento asigna a la Unidad de Tecnología e Informática.

La Unidad de Tecnología e Informática cumplirá lo indicado en los numerales que anteceden, con observancia de las disposiciones de control constantes del artículo 104 del Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, codificación publicada en el Registro Oficial Suplemento 888 de 23 de noviembre de 2016.

Art. 13.- Mantenimiento.- La Unidad de Tecnología e Informática elaborará un plan de mantenimiento preventivo y correctivo de los bienes, equipos y sistemas informáticos que dispone la Institución, contemplando en la planificación institucional los recursos necesarios para su contratación.

La Unidad de Tecnología e Informática se encargará de gestionar los mantenimientos planificados con hora de inicio, fin, impacto y responsables, y pondrá previamente en conocimiento de los servidores custodios de los bienes informáticos, para que los entreguen o permitan su mantenimiento.



En caso de producirse daños o desperfectos en los equipos, sistemas o recursos informáticos, el servidor responsable y custodio de los mismos informará lo sucedido, oportunamente y por escrito, a la Unidad de Tecnología e Informática para que se tomen los correctivos necesarios o en su defecto se solicite la respectiva reparación o cambio de los mismos, según corresponda.

La Unidad de Tecnología e Informática establecerá controles apropiados para realizar mantenimientos programados y emergentes; y, conservará los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas generadas.

Los mantenimientos se realizarán únicamente con personal autorizado y calificado.

El plan de mantenimiento se ajustará a las disposiciones del artículo 103 del Reglamento general para la administración, utilización, manejo y control de los bienes y existencias del sector público, codificación publicada en el Registro Oficial Suplemento 888 de 23 de noviembre de 2016; y a las disposiciones del principio de vigencia tecnológica que establece el capítulo III del Título III de la codificación y actualización de las resoluciones emitidas por el Servicio Nacional de Contratación Pública, de 31 de agosto de 2016.

Art. 14.- Devolución.- Las devoluciones de los equipos o sistemas informáticos por cualquier razón que esta sea, tendrá que realizarse de acuerdo al siguiente procedimiento:

- a. Los bienes o equipos informáticos tienen que ser entregados por parte del custodio al responsable o delegado de la Unidad de Tecnología e Informática, quien en coordinación con Servicios Generales procederá a revisar el estado y condiciones del bien, para con posterioridad suscribir la o las actas de devolución y se actualizará la hoja de vida del bien.
- b. En el caso de encontrar novedades en la devolución de los equipos se reportará a la Dirección Administrativa Financiera para que tome los correctivos o acciones pertinentes.
- c. En caso que la devolución del bien se deba a motivos de ausencia temporal, definitiva o cambios al interior de la Institución del servidor custodio, en forma previa este deberá entregar a su jefe inmediato y a la Unidad de Tecnología e Informática un respaldo magnético completo de la información constante en el mismo, esta acción será respaldada por la firma de un acta entrega de información digital, la cual tendrá que ser firmada por el funcionario saliente, un servidor de la Unidad de Tecnología e Informática y el jefe inmediato superior.
- d. El respaldo de la información será de responsabilidad de la Unidad de Tecnología e Informática y del propietario de la información, para lo cual se determinarán los procedimientos de resguardo y contención de la información en el Instructivo que aprobará la máxima autoridad a petición del Comité de Seguridad de la Información.
- e. La Unidad de Tecnología e Informática deberá proceder a formatear y tener listos los equipos para asignarlos a nuevos servidores que así lo requieran.

Sección II

Procedimiento de creación, modificación y eliminación de usuarios

Art. 15.- Procedimiento.- A fin de garantizar la seguridad de la información contenida en los sistemas informáticos de la Institución, para crear un nuevo usuario, el mismo tiene que ser aprobado por la Dirección Administrativa Financiera, quien autorizará los perfiles de usuario y atribuciones, según sea el caso, y dispondrá a la Unidad de Tecnología e Informática dicha creación, modificación o eliminación previa comunicación por escrito.

No se crearán cuentas anónimas o de invitado.

Art. 16.- Eliminación.- Para proceder a eliminar un usuario, la Unidad de Administración de Talento Humano tiene la obligación de informar y enviar dicho pedido para su aprobación a la Dirección Administrativa Financiera, quien dispondrá a la Unidad de Tecnología e Informática la eliminación del usuario en los sistemas en los cuales se registró, teniendo además que respaldar la información del servidor, según sea el caso.



La Unidad de Tecnología e Informática no almacenará información en los servidores institucionales referente a perfiles de usuario (Mis documentos, Escritorio, etc.), motivo por el cual, la responsabilidad de la información que se genere y custodie en cada equipo institucional será directamente del jefe inmediato del servidor que cese en sus funciones. La Unidad de Tecnología e Informática dará soporte técnico, de ser el caso, para el respaldo de la información existente que reposa en el computador, sin discretización de la misma.

Art. 17.- Contraseña de Usuarios.- Para todo aspecto referente al manejo de contraseñas deberá ser aplicado el artículo 54 del presente instrumento, haciendo hincapié que las contraseñas administradas en los servicios de correo electrónico y de perfiles de equipo son centralizadas y encriptadas en el servidor de cómputo donde reside el servicio de Directorio Activo (Active Directory), herramienta que es continuamente actualizada para mitigar o reducir problemas de seguridad. En caso de emergencia de seguridad el personal técnico tendrá la autorización para solicitar el cambio de contraseñas sin previo aviso, de forma inmediata y una vez mitigado el problema entregará un informe de los acontecimientos suscitados.

Art. 18.- Manejo de Contraseñas.- Todo servidor del Tribunal Contencioso Electoral o tercero desde el momento que ingrese a prestar sus servicios en la Institución, deberá firmar un "Acuerdo de Confidencialidad", el mismo que incluirá responsabilidad en el uso de claves y medios electrónicos institucionales, lo que determinará que son los únicos responsables de todas las actividades realizadas con sus claves asignadas para el servicio de telefónica fija o celular a su cargo, cuentas de acceso a su buzón de correo electrónico, servicio de Internet que hayan sido entregados como herramientas de trabajo.

Art. 19.- Utilización excepcional de cuentas de usuario.- La utilización de las cuentas de usuario no deben proporcionarse a personas que no sean servidores públicos del Tribunal Contencioso Electoral, a excepción de aquellos que estén debidamente autorizados por la Máxima Autoridad.

Sección III

Seguridad, protección y cuidado

Art. 20.- Seguridad.- A fin de garantizar la seguridad de los bienes, equipos, sistemas y recursos informáticos de la Institución todo usuario observará las siguientes normas:

- a. Será responsabilidad de la Unidad de Tecnología e Informática gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
- b. Definir claramente el personal responsable de la administración de los permisos de acceso a la información por cada Despacho de Juez, Dirección o Unidad.
- c. Definir el administrador de accesos que debe controlar los perfiles y roles.
- d. Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (precautelando la debida confidencialidad).
- e. La Unidad de Tecnología e Informática tendrá la obligación de recomendar y controlar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales difíciles de descifrar, es decir, que cumplan una complejidad media o alta.
- f. La Unidad de Tecnología e Informática gestionará el cambio periódico de contraseñas de los usuarios.
- g. Evitar contraseñas en blanco o que vienen por defecto según el sistema del fabricante del producto, puesto que son fácilmente descifrables.
- h. La Unidad de Tecnología e Informática tendrá la obligación de generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología.
- i. Todo usuario registrado será responsable de proteger su nombre de usuario, contraseña y demás seguridades que sean implementadas por la Institución, de cualquier acceso no autorizado, para lo cual considerará que las cuentas institucionales no se pueden compartir ni delegar y que debe proteger su contraseña y cambiarla regularmente.



- j. Tener especial cuidado en el uso y manejo de las claves y seguridades empleadas para acceder a los servicios tecnológicos de la Institución.
- k. Se prohíbe el uso no autorizado de un nombre de usuario o claves de un usuario distinto al propiamente registrado.
- l. En caso de la utilización de un nombre de usuario no autorizado, el afectado comunicará inmediatamente tal hecho a la Unidad de Tecnología e Informática, a fin de adoptar los correctivos que sean del caso.
- m. Todo usuario respetará las claves, seguridades o contraseñas de los demás usuarios y funcionarios de la Institución, que por el ejercicio de sus funciones pudieren llegar a su conocimiento, como parte de su trabajo o de forma accidental. Si se diera algún caso de obtención de contraseña de otro usuario se deberá comunicar este evento a la Unidad de Tecnología e Informática, a fin de adoptar los correctivos que sean del caso.
- n. Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie fecha, creación, eliminación, suspensión, activación o eliminación del acceso al igual que cada usuario dispondrá de los servicios de acceso que han sido asignados.
- o. La Unidad de Tecnología e Informática está en la obligación de mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio, software o sistema operativo, sistema de gestión de base de datos y aplicaciones.
- p. Evidenciar documentadamente que cada activo de información tecnológica tenga definido los niveles de acceso basado en perfiles y permisos, a fin de determinar qué privilegios se deben asignar según las actividades de los usuarios y las necesidades de la Institución y sus funciones.
- q. No se podrá modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos; en este sentido, todo usuario interno o externo respetará las políticas implantadas por la Institución referentes a la asignación y privilegios de acceso a los servicios tecnológicos.
- r. El acceso a los servicios con privilegios especiales se realizará previa autorización de la Máxima Autoridad o de la Dirección Administrativa Financiera y será de responsabilidad de la Unidad de Tecnología e Informática mantener actualizado el listado de los funcionarios con acceso a dichos servicios.
- s. No se podrá modificar, alterar, sustituir, remplazar, bloquear, restringir o almacenar información institucional con el propósito de impedir que un usuario pueda acceder o disponer de ella sin la debida autorización.
- t. En caso de que algún usuario asigne contraseñas o codifique la información institucional a fines de evitar que otros usuarios puedan acceder o disponer de ella, éste facilitará la información necesaria para lograr el acceso a los archivos o en su defecto se impondrán las medidas disciplinarias que correspondan frente a este hecho. La Institución, a través de la Unidad de Tecnología e Informática, estará facultada para decodificar la misma o restituirla a su condición original y reportar cualquier novedad sobre su tratamiento.
- u. La información generada por los servidores en el ejercicio de sus funciones o actividades laborales en la Institución deberá permanecer siempre almacenada en los equipos informáticos asignados por la Unidad de Tecnología e Informática. Está prohibido el almacenamiento en equipos o dispositivos que no reposen o sean de propiedad del Tribunal Contencioso Electoral, salvo el caso de que se traten de respaldos de información personal.
- v. El acceso a las oficinas, infraestructura, bienes, equipos y sistemas informáticos que dispone la Institución será coordinado únicamente por intermedio de la Unidad de Tecnología e Informática, a través de los servidores que pertenecen a esta unidad o por autorización de la Máxima Autoridad o la Dirección Administrativa Financiera. Los demás servidores podrán acceder a los mismos únicamente con el acompañamiento o aprobación de la Unidad de Tecnología e Informática.
- w. Queda prohibido congestionar enlaces de comunicaciones o sistemas informáticos mediante la ejecución de programas maliciosos o de reproducción de radio, video, transferencia de archivos o programas que sean para uso personal y que no sean necesarios para el cumplimiento de las labores institucionales.
- x. La información institucional que se genere, utilice, procese, comparta y almacene en cualquier medio electrónico o escrito, clasificada como pública o pública confidencial o reservada, deberá manejarse y utilizarse conforme lo determina el presente Reglamento u otros instrumentos institucionales, a fin de definir por parte de la Unidad de Tecnología e Informática los procesos,



procedimientos y medios tecnológicos que permitan garantizar la confidencialidad, integridad y disponibilidad de esa información institucional, en los medios y el tiempo que su legitimidad lo requiera.

- y. La Unidad de Tecnología e Informática establecerá protocolos de uso, manejo y seguridad de la información institucional, con la finalidad de garantizar y precautelar la debida confidencialidad y reserva de la misma.

Art. 21.- Equipos periféricos.- A fin de garantizar la protección y cuidado de los bienes o equipos periféricos (terminales, impresoras, dispositivos auxiliares para computadoras, etc.), todo usuario observará las siguientes normas:

- a. Únicamente el personal autorizado por la Unidad de Tecnología e Informática podrá manipular, sustituir, instalar y configurar los equipos tecnológicos, de computación o sistemas informáticos.
- b. En caso de que el usuario detecte problemas en el funcionamiento de los bienes, equipos o sistemas informáticos de la Institución, deberá notificar inmediatamente a la Unidad de Tecnología e Informática para que se proceda con la revisión de los mismos, a fin de que se tomen los correctivos del caso o se envíen para la respectiva revisión o reparación, según corresponda.
- c. No se podrá tener o consumir alimentos ni bebidas en las áreas de trabajo donde se encuentren localizados los bienes, equipos o sistemas informáticos.
- d. Cualquier movimiento, traspaso o reubicación de los bienes o equipos informáticos de la Institución, así como de sus periféricos deberá ser coordinado con el personal de la Unidad de Tecnología e Informática, para lo cual se solicitará a la Dirección Administrativa Financiera la elaboración del documento de traspaso correspondiente.
- e. Al finalizar sus labores diarias, cada usuario deshabilitará su clave de acceso del terminal o computadora y apagará todos los equipos electrónicos en su área de trabajo, o cuando así se lo requiera.

Sección IV

Equipos de reproducción

Art. 22.- Utilidad.- El uso de equipos de reproducción como impresoras, copiadoras, escáneres, etc., serán única y exclusivamente para fines estrictamente laborales o relacionados con las funciones y actividades desempeñadas en la Institución; se imprimirá los documentos cuando fuere estrictamente necesario.

Art. 23.- Uso racional.- Será obligatorio el uso adecuado, racional y estrictamente necesario de los equipos de reproducción, al momento de realizar la impresión o copiado de documentos, para lo cual la Unidad de Tecnología e Informática realizará un seguimiento, control y llevará un reporte de las impresiones realizadas por cada una de las áreas o unidades, con el fin de dar cumplimiento a esta disposición.

Art. 24.- Consumibles.- Los consumibles de las impresoras o copiadoras deberán ser cambiados o reemplazados únicamente por el personal de la Unidad de Tecnología e Informática, previa solicitud del área requirente y constatación del agotamiento de los mismos, entre otros: toners, cintas de impresora zebra, rodillos, fotoconductores de impresoras multifunción y aquellos que de acuerdo al avance tecnológico sean considerados como tales.

Art. 25.- Daños y desperfectos.- En caso de producirse daños o desperfectos en los equipos de reproducción, el servidor responsable y custodio de los mismos informará lo sucedido oportunamente y por escrito a la Unidad de Tecnología e Informática para que se tomen los correctivos necesarios o en su defecto se solicite la respectiva reparación y cambio de estos.

Sección V

Software

Art. 26.- Adquisición de software.- Previo a iniciar el proceso de contratación, toda unidad requirente deberá solicitar a la Unidad de Tecnología e Informática la validación de las especificaciones técnicas del



caso.

Todo software propietario que se utilice en los equipos informáticos del Tribunal Contencioso Electoral deberá ser adquirido a nombre de la Institución y contar obligatoriamente con su licencia legal.

Art. 27.- Contratos con terceros.- Para la adquisición de equipos informáticos de escritorio o equipos portátiles, equipos de impresión, equipos de telecomunicaciones y software de terceros, se contemplará una cláusula en el respectivo contrato que establezca el procedimiento para la obtención de datos, programas fuentes, manuales y documentación asociada por imprevistos que pudiera sufrir el proveedor y que provoquen la culminación de sus servicios, procedimiento que deberá contemplarse en los términos de referencia elaborados por el área requirente del bien o servicio.

Art. 28.- Software recibido para prueba.- En caso que la Institución reciba software de terceros para ser probados y evaluados por el Tribunal Contencioso Electoral, se deberá suscribir un acta en donde consten las funcionalidades generales del sistema, el cual se implementará en un ambiente tecnológico alterno al ambiente final o de producción institucional.

Art. 29.- Instalación de software.- La Unidad de Tecnología e Informática es responsable de la homologación inicial, instalación y/o eliminación de cualquier tipo de software en los equipos centralizados de procesamiento y/o en cualquiera de los equipos conectados o no a la red de datos del Tribunal Contencioso Electoral.

Art. 30.- Desarrollo interno de software.- Todo software desarrollado por la Unidad de Tecnología e Informática será de propiedad del Tribunal Contencioso Electoral, para lo cual la Dirección de Asesoría Jurídica deberá registrarlo a nombre de la Institución, conforme las disposiciones de propiedad intelectual vigentes.

Art. 31.- Transferencia y donaciones a terceros.- Toda transferencia a terceros de software desarrollado por el Tribunal Contencioso Electoral será autorizada por la Máxima Autoridad y contará con el correspondiente respaldo legal.

En toda donación de equipos informáticos se identificarán detalladamente todos los recursos de software que se incluyen en la operación.

Art. 32.- Control de licencias.- La Unidad de Tecnología e Informática elaborará un inventario de las versiones de software instaladas en todos los equipos informáticos del Tribunal Contencioso Electoral, el cual será actualizado periódicamente de manera trimestral.

Capítulo III SERVICIO DE TELEFONIA IP

Sección I Uso del servicio

Art. 33.- Utilidad.- El servicio de telefonía IP es una herramienta de trabajo institucional, por lo que todo servidor o servidora deberá dar un uso adecuado a este servicio, precautelando que el tiempo utilizado sea el estrictamente necesario para el cumplimiento de sus labores y objetivos de la Institución.

Art. 34.- Habilitación.- El servidor no requerirá de claves, códigos o autorizaciones especiales para el uso de llamadas permitidas (locales, provinciales, regionales y llamadas a líneas gratuitas) a excepción de las llamadas a celular e internacional. En caso de que se detecte el uso anormal de las claves entregadas, con el fin de adoptar medidas pertinentes, previa autorización de la Máxima Autoridad, se deberá recabar la información necesaria solicitando los registros de llamadas a la Unidad de Tecnología e Informática, justificando el motivo de dicha solicitud.



Art. 35.- Prohibiciones.- Se prohíbe a los servidores del Tribunal Contencioso Electoral:

- a. Mover o crear extensiones con o sin clave.
- b. Mover los teléfonos a unidades o despacho distintos a los entregados.
- c. Difundir y utilizar las claves de acceso, entregadas únicamente a los servidores autorizados por la Máxima Autoridad.
- d. Utilizar este servicio para actividades ajenas a la Institución.

Sección II

Control

Art. 36.- Consumo y debido uso.- La Unidad de Tecnología e Informática realizará un control trimestral del servicio, uso y consumo de la telefonía IP, verificando además que el uso de las claves asignadas a servidores específicos no tengan un acceso diferente al autorizado; y, de ser el caso, podrá limitar el acceso a dichas claves, previa autorización del titular de la Dirección Administrativa Financiera conforme a las necesidades del servidor.

Art. 37.- Supervisión.- La Dirección Administrativa Financiera vigilará, sobre la base de un reporte mensual de la Unidad de Tecnología e Informática, que los gastos por consumo de telefonía IP, especialmente los servicios de larga distancia nacional e internacional que demandan cargos por interconexión con otras operadoras telefónicas, se reduzcan al mínimo indispensable, tendiendo siempre a la utilización óptima del servicio e informando de cualquier anomalía a la Máxima Autoridad o su delegado, a fin de que establezcan los correctivos necesarios.

Art. 38.- Listado.- La Dirección Administrativa Financiera asignará y mantendrá actualizados los listados de los responsables de las extensiones y claves, de ser el caso, de la telefonía IP, y realizará el monitoreo del uso y el tipo de accesos requeridos y autorizados.

Art. 39.- Verificación.- La Unidad de Administración de Talento Humano notificará a la Unidad de Tecnología e Informática los cambios de puestos, permisos, traslados y cesación de funciones de los servidores del Tribunal Contencioso Electoral, a fin de proceder con las medidas necesarias que permitan el control de las claves, abiertas al servicio de telefonía IP.

La notificación a la que se refiere el inciso anterior no podrá ser superior a las 48 horas de expedido el acto administrativo en cualquiera de los casos determinados en el inciso precedente.

Sección III

Seguridades

Art. 40.- Autorización.- La Dirección Administrativa Financiera, previa autorización de la Máxima Autoridad o su delegado, dispondrá a la Unidad de Tecnología e Informática asignar y entregar una clave personal para realizar llamadas a celular e internacionales a los servidores designados para tal efecto, quienes serán los únicos responsables del manejo de la misma.

Art. 41.- Actualización.- Las claves de acceso se actualizarán periódicamente según lo determine la Dirección Administrativa Financiera y cuando lo solicite el usuario.

Sección IV

Acciones correctivas

Art. 42.- Suspensión.- La Dirección Administrativa Financiera podrá suspender los accesos a los servicios de telefonía IP en los casos de solicitud motivada y expresa del servidor responsable de la clave, por considerarse innecesario el servicio o por exceso no justificado del consumo, así como por disposición expresa de las autoridades de la Institución.

Art. 43.- Responsabilidad.- De comprobarse que el servicio de telefonía IP está siendo utilizado por el



servidor en actividades ajenas a las del Tribunal Contencioso Electoral, se ejercerá por parte de la Institución el derecho a cobrarle los valores incurridos, previo informe motivado de la Unidad de Tecnología e Informática.

Art. 44.- Acceso no autorizado.- De encontrarse o verificarse el servicio telefónico con acceso no autorizado, el custodio de la clave deberá explicar su indebida utilización a fin de que la Unidad de Tecnología e Informática tome las medidas o acciones preventivas o correctivas que se ameriten.

Art. 45.- Capacitación.- La Unidad de Administración de Talento Humano conjuntamente con la Unidad de Tecnología e Informática brindará capacitación a todo el personal y en particular al personal encargado de atender llamadas telefónicas respecto del uso de los dispositivos, la cortesía al público, amabilidad y diligencia con que deben hacerlo, con el objeto de precautelar los recursos y la imagen institucional.

Capítulo IV

SERVICIO DE CORREO ELECTRÓNICO

Sección I

Uso del servicio

Art. 46.- Utilidad.- Este servicio deberá utilizarse exclusivamente para el ejercicio de las funciones propias de cada servidor del Tribunal Contencioso Electoral, por lo tanto se prohíbe el envío de mensajes individuales o en cadena ajenos al ámbito de gestión de la Institución.

Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información o archivo adjunto al mismo.

Art. 47.- Medidas de seguridad.- Son todos aquellos mecanismos tecnológicos e informáticos que se aplicarán a todo el servicio de correo electrónico institucional en la red interna y externa que es utilizada por servidores del Tribunal Contencioso Electoral para el envío y recepción de mensajes electrónicos, como herramienta para desarrollo de las actividades que realizan en el marco de sus funciones. Estas medidas tienen por finalidad evitar riesgos en la transmisión de información mediante el correo electrónico institucional provocados por un inadecuado manejo, para lo cual se deberán aplicar las siguientes normas:

- a. Las cuentas de correo electrónico institucional podrán ser monitoreadas y respaldadas por parte de la Unidad de Tecnología e Informática para efectos de supervisión administrativa y determinar el mal uso de la cuenta de ser el caso. Los mensajes deben mantenerse en carpetas personales, lo que permitirá archivar la información de acceso exclusivo del usuario, para ello se definirá un límite de espacio máximo a destinarse para este efecto sin que dicha información pueda ser compartida con otros usuarios.
- b. La o las cuentas de correo electrónico institucional deberán estar asociadas a una única cuenta de usuario, lo cual realizará la Unidad de Tecnología e Informática.
- c. Toda la información debe ser gestionada de forma centralizada y no en las estaciones de trabajo de los usuarios, como una medida de seguridad de la información, lo cual realizará la Unidad de Tecnología e Informática y se informará de su cumplimiento a las unidades de la Institución.
- d. El correo electrónico contará con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error. La Unidad de Tecnología e Informática, de ser el caso, informará de los errores presentados en el envío del mensaje a las unidades de la Institución.

Art. 48.- Conexión en red.- El acceso al correo electrónico únicamente se realizará a través un navegador Web sin necesidad de realizar descargas de mensajes al propio ordenador y por medio de protocolos de sincronización POP3 e IMAP, excepto para la gestión de correos en dispositivos móviles y tabletas. No se autoriza el uso de cualquier software gestor de correo electrónico en los computadores institucionales diferente a un navegador Web.



Sección II
Responsabilidades

Art. 49.- Responsabilidad del usuario.- Son responsabilidades del usuario:

- a. Administrar la información respecto a la recepción de correos al destinatario de la información.
- b. Verificar la carpeta de correos spam y eliminarlos directamente sin abrirlos en caso de existir.
- c. Verificar mensajes de alerta de exceso del tamaño de su buzón.
- d. Notificar a la Unidad de Tecnología e Informática en caso de permisos, vacaciones o ausencia temporal para establecer el respectivo mensaje de notificación a los destinatarios de correo.
- e. Depurar el buzón de su correo, con el fin de no saturar el espacio asignado a su cuenta de correo.
- f. En caso de llegar al límite del tamaño de su buzón, notificar a la Unidad de Tecnología e Informática para realizar un respaldo de la cuenta e inmediatamente el usuario procederá a eliminar los correos que crea pertinente en fin de liberar espacio en la cuenta.
- g. Todo usuario es responsable por el uso y manipulación de los mensajes con origen desconocido y asume la responsabilidad por las consecuencias que pueda ocasionar a los recursos tecnológicos e informáticos la ejecución de los archivos adjuntos. En estos casos, no debe contestar dichos mensajes y enviará una copia a la Unidad de Tecnología e Informática para que efectúe el seguimiento y análisis correspondiente, o en su defecto eliminarlos.

Art. 50.- Responsabilidad de la Unidad de Tecnología e Informática.- Son sus responsabilidades:

- a. Mantener la seguridad por medio de un antivirus actualizado y análisis de tráfico generado dentro de la Institución.
- b. Asegurar la descarga de correos antiguos a un repositorio local para la limpieza del buzón.
- c. Generar reportes de uso de correo, de acuerdo con la petición de las autoridades, en razón de la propiedad intelectual de la Institución respecto de la información contenida en los equipos y correo electrónico. Estos reportes se realizarán de conformidad con las disposiciones legales vigentes.

Sección III
Seguridades

Art. 51.- Pie de firma.- El formato de pie de firma en los correos electrónicos mantendrá el formato de imagen (jpeg) asignado por la Unidad de Comunicación Social a cada uno de los servidores y contendrá necesariamente: nombres y apellidos completos, denominación del cargo que ocupa, descripción del Despacho, Dirección o Unidad donde labora, nombre y teléfono de la Institución y dirección electrónica del sitio Web Institucional. Cada servidor es responsable de mantener y difundir en sus correos la firma actualizada. No se podrá incluir firmas personalizadas.

Art. 52.- Permisos de acceso.- Todos los servidores del Tribunal Contencioso Electoral, así como terceros que interactúan con la Institución, tendrán permisos de acceso única y exclusivamente a los recursos informáticos para los que han sido debidamente asignados por autoridad competente; en este contexto, las actividades descritas a continuación se desarrollarán de la siguiente manera:

- a. Las listas de distribución públicas serán creadas solamente por la Unidad de Tecnología e Informática, conforme a lo señalado en el Estatuto Orgánico de Gestión de Procesos del Tribunal Contencioso Electoral y a los requerimientos de cada una de las unidades que lo conforman.
- b. En caso de necesitar la creación o modificación de una lista de distribución se deberá remitir un correo electrónico a la Unidad de Tecnología e Informática, solicitando lo correspondiente.
- c. El acceso a las listas de distribución solo se realizará desde cuentas de correo internas de la Institución que tengan la autorización debida por parte del órgano competente.
- d. Los correos enviados hacia las listas de distribución deben tener archivos adjuntos con un tamaño máximo de 6 MB y serán enviados con un tiempo promedio de una hora y media entre cada uno de los envíos masivos.



- e. Las cuentas de correo electrónico institucional permitirán el envío y la recepción de mensajes asociados a esta dirección única "nombre.apellido@tce.gob.ec". Para acceder a una cuenta de correo se requiere de la dirección única y contraseña, las cuales son almacenadas en un repositorio de ACTIVE DIRECTORY. Estas contraseñas serán gestionadas directamente por el servidor luego de una asignación con clave temporal por parte de la Unidad de Tecnología e Informática y su uso se limitará al cumplimiento de las funciones institucionales.
- f. La cuenta del correo electrónico individual será intransferible, con acceso exclusivo y personal del servidor correspondiente, además podrán generarse cuentas para uso especial, atendiendo a las necesidades de cada una de las unidades que así lo requieran a la Unidad de Tecnología e Informática.
- g. Cuando se configure la cuenta del servidor, se requerirá que este cambie la clave de acceso por medio del inicio de sesión del sistema operativo Windows vigente, con lo que se brinda mayor seguridad para que solo el titular de la cuenta de correo la conozca y use.
- h. Luego de configurar la cuenta de correo electrónico, se habilitará la opción de "Archivar" el correo histórico, lo que permitirá administrar la información del usuario y evitar que se sature la bandeja de entrada.
- i. Las creaciones y eliminaciones de cuentas de los servidores se realizarán siguiendo los lineamientos de este Reglamento para la creación y eliminación de usuarios, mediante solicitud a la Unidad de Tecnología e Informática por parte de la Unidad de Administración de Talento Humano, con los datos personales como nombres completos, número de cédula y puesto en la Institución.
- j. En caso de olvido o bloqueo de la contraseña, el usuario coordinará la habilitación de la cuenta con la Unidad de Tecnología e Informática.

Art. 53.- Tipos de Cuentas.- Se establecen tres tipos de movimientos de cuentas de usuarios bajo los siguientes parámetros:

- a. Alta de perfil de usuario: cuando el usuario ingresa a la Institución o requiere acceso a un nuevo sistema.
- b. Modificación de perfil de usuario: cuando el usuario requiere nuevos permisos de acceso a igual información y/o a nueva información.
- c. Baja de perfil de usuario: cuando el usuario no accede más de manera permanente al sistema o se desvincula del Tribunal Contencioso Electoral.

Art. 54.- Contraseña.- La contraseña tiene por objeto garantizar que únicamente el usuario, de acuerdo a su perfil y funciones, tenga acceso a la información pertinente. Se gestionará según las siguientes reglas:

- a. Las contraseñas deben ser de carácter personal e intransferible, deberán mantenerse y manejarse en secreto por el usuario.
- b. Se prohíbe a los servidores del Tribunal Contencioso Electoral dar a conocer su contraseña a terceras personas, quien así lo hiciere, será legalmente responsable de las actividades que se realicen con su identificación de usuario (ID) y contraseña.
- c. De los cuatro (4) grupos de caracteres (mayúsculas, minúsculas, números y caracteres especiales), la clave al menos deberá contener seis (6) caracteres, y como mínimo tres (números), un (1) carácter especial y tres (3) letras.
- d. En caso de que el usuario sospeche que su contraseña ha sido comprometida deberá solicitar inmediatamente su cambio a la Unidad de Tecnología e Informática.
- e. En caso de olvido o bloqueo de su contraseña, el usuario deberá coordinar el restablecimiento de la cuenta con la Unidad de Tecnología e Informática.
- f. Por regla general las contraseñas deberán ser cambiadas periódicamente cada noventa (90) días, de acuerdo con la importancia y la sensibilidad de la información a la que se tiene acceso.
- g. Los servidores del Tribunal Contencioso Electoral deberán utilizar contraseñas que no resulten obvias, fáciles de adivinar o descubrir, o no sean predecibles para un posible atacante, tales como: nombre o apellidos del usuario, fechas o nombres de personas allegadas, secuencias de números repetidos, entre otros. Para que las contraseñas cumplan con su función de seguridad de la



información, deberán tener una longitud mínima de 6 caracteres alfanuméricos (número, letras y/o caracteres especiales combinados).

- h. La contraseña no deberá contener el nombre de la cuenta que use para acceder al computador asignado.
- i. La contraseña no deberá ser la misma utilizada en los tres (3) últimos cambios de contraseñas anteriores.

Art. 55.- Respaldo.- Si el servidor del Tribunal Contencioso Electoral requiere obtener un respaldo de sus correos en un archivo independiente, deberá ser autorizado por el jefe inmediato, esto es también aplicable para casos en que un servidor del Tribunal Contencioso Electoral se separe de la Institución, para lo cual se coordinará con la Unidad de Tecnología e Informática.

Art. 56.- Tamaño del buzón.- El tamaño estándar es de 2 GB, este podrá ser ampliado por solicitud expresa y tomando en cuenta también el cargo del servidor del Tribunal Contencioso Electoral, fundamentado bajo los siguientes parámetros:

- a. Autoridades, máximo hasta 4 GB.
- b. Directores y Asesores, máximo hasta 3 GB.

Art. 57.- Responsabilidad.- El proceso de respaldo de los buzones de correo electrónico de los servidores del Tribunal Contencioso Electoral tiene un carácter de responsabilidad compartida entre el usuario, quien conoce que ha respaldado o no, y el personal de soporte técnico, que realice la descarga de sus correos personales e institucionales al equipo asignado. En caso de requerir este servicio de respaldo se lo solicitará a la Unidad de Tecnología e Informática.

Art. 58.- Administración de correos asociados.- Los correos de los sistemas asociados que tienen buzones de recepción de la ciudadanía deberán ser administrados por el servidor del Tribunal Contencioso Electoral del área correspondiente y se ejecutará el mismo procedimiento en el equipo asignado para esta labor.

Art. 59.- Revisión y control.- De existir causa justificada por escrito y so pena de sanciones administrativas, civiles y penales de quien lo solicite, las cuentas de correo electrónico serán susceptibles de revisión por parte de Auditoría Interna y de la Unidad de Tecnología e Informática, previo el conocimiento y autorización de su titular en caso de que la relación laboral este vigente.

Art. 60.- Envío de información masiva.- Únicamente los correos institucionales emitidos por la Unidad de Comunicación Social y la Unidad de Tecnología e Informática del Tribunal Contencioso Electoral y aquellos que la Dirección Administrativa Financiera autorice, contendrán comunicados generales mediante el envío masivo por las listas de distribución existentes.

Los envíos de mensajes masivos por correo electrónico solo podrán contener información de interés general y relacionada con las actividades o funciones propias de la Institución.

Queda totalmente prohibida cualquier difusión masiva de anuncios electrónicos de tipo personal.

Art. 61.- Prevención de virus y programas maliciosos.- La Unidad de Tecnología e Informática utilizará programas que monitoreen el accionar de los virus informáticos tanto para los mensajes de correo como para todos los archivos adjuntos previamente a su ejecución, para lo cual:

- a. Instalará y vigilará la actualización del software de antivirus y código malicioso.
- b. Mantendrá los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.
- c. Revisará periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Institución.
- d. Verificará antes de su uso la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables.



- e. Concienciará al personal de la Institución acerca del problema de los virus y como proceder frente a los mismos.
- f. Se prohíbe introducir en los computadores personales cualquier tipo de medio de almacenamiento sin que previamente haya sido revisado por el software antivirus de la Institución, para descartar la presencia de virus o cualquier otro programa dañino.
- g. Se prohíbe conectar en la red institucional cualquier equipo de computación y/o dispositivo móvil sin la autorización y la revisión previa de la Unidad de Tecnología e Informática.
- h. Se prohíbe grabar en los dispositivos de almacenamiento de los equipos de computación personales cualquier tipo de archivo de dudosa condición o calidad que pueda ocasionar daños. Esto aplica a archivos procedentes de Internet o introducidos al PC por medio de dispositivos de almacenamiento externos (ejemplo: disco duro externo, flash memories o de cualquier otra índole) sin que se tenga la certeza de que están libres de códigos maliciosos.
- i. El usuario verificará regularmente que su equipo de computación disponga de software antivirus actualizado. De no contar con dicha herramienta o en caso de duda, está obligado a solicitar a la Unidad de Tecnología e Informática su inmediata actualización.
- j. El usuario deberá abstenerse de abrir, responder o reenviar mensajes de correo electrónico que no provengan de fuentes conocidas y seguras, y descargar anexos enviados por correo electrónico que puedan ser fuente de virus o similares o cuya procedencia y características desconozca.
- k. El usuario en caso de presumir o evidenciar la presencia de virus o similares en su equipo de computación, deberá de inmediato salir de los programas que al momento esté ejecutando, apagar el computador, notificar a la Unidad de Tecnología e Informática a través de correo electrónico, asegurándose que su requerimiento ha sido registrado y atendido eficazmente.

Art. 62.- Notificación de errores.- Todo sistema tendrá implementadas facilidades automáticas que permitan al usuario ser notificado con error con la recepción de un mensaje, en caso de que dicho mensaje no sea recibido correctamente por el destinatario seleccionado, notificación que describirá detalladamente el motivo del error.

Art. 63.- Encriptación y firma electrónica.- Para el uso de información sensible, envío y conservación, se implementará la facilidad de encriptación de datos y firma electrónica, en la medida que lo permitan los sistemas utilizados.

Capítulo V

DISPOSITIVOS PORTÁTILES

Sección I

Webmail

Art. 64.- Definición.- Opción tecnológica mediante la cual se puede efectuar una conexión remota al buzón de correo institucional, esta conexión puede ser realizada por medio de cualquier navegador existente siendo recomendable utilizar Mozilla Firefox para asegurar la completa funcionalidad.

Art. 65.- Responsabilidades del usuario.- Son responsabilidades de usuario las siguientes:

- a. Acceder al webmail a través de un computador libre de programas que amenacen la seguridad de la cuenta.
- b. Tomar las precauciones necesarias si utiliza esta funcionalidad desde un computador público.
- c. Asegurar que la sesión sea cerrada al momento de dejar de utilizar esta funcionalidad.

Art. 66.- Responsabilidades de la Unidad de Tecnología e Informática.- Son sus responsabilidades las siguientes:

- a. Mantener la seguridad por medio de una solución de seguridad para garantizar la protección del servidor de correo.
- b. Garantizar la disponibilidad del servicio en un 96% de uptime mensual.



Sección II
Dispositivos Móviles

Art. 67.- Definición.- Son herramientas, dispositivos o equipos tecnológicos (tablets, smartphones, computadores portátiles) que permiten a los servidores del Tribunal Contencioso Electoral gestionar su cuenta de correo y agenda electrónica en cualquier lugar; para ello se utilizarán dispositivos portátiles que brinden estas ventajas.

Art. 68.- Responsabilidades del usuario.- Son responsabilidades de usuario las siguientes:

- a. Utilizar redes de comunicación seguras en el caso de existir una conexión mediante WiFi.
- b. El uso del dispositivo institucional móvil debe ser personal y procurar que personas no autorizadas no tengan acceso al mismo.
- c. En caso de pérdida, robo o hurto del dispositivo institucional móvil, informar al personal de sistemas para cambiar la contraseña de la cuenta respectiva.
- d. Mantener el dispositivo institucional móvil libre de programas peligrosos que puedan atentar contra la información institucional.
- e. Mantener actualizado tecnológicamente el dispositivo institucional móvil.
- f. Revisar de forma continua los correos enviados y recibidos desde el dispositivo institucional móvil.

Art. 69.- Responsabilidades de la Unidad de Tecnología e Informática.- Son sus responsabilidades las siguientes:

- a. Mantener garantías orientadas a una óptima seguridad, a través de soluciones precisas e inmediatas a fin de lograr protección del servidor institucional de correo.
- b. Garantizar la disponibilidad del servicio en un 96% de uptime mensual.
- c. Monitorear periódica e indistintamente el uso y manejo de los recursos tecnológicos institucionales a fin de verificar su correcto uso, y en caso de encontrar novedades, notificar inmediatamente lo ocurrido al titular de la Dirección Administrativa Financiera.

Capítulo VI
SERVICIO DE INTERNET

Sección I
Uso del servicio

Art. 70.- Reglas sobre el uso.- Internet es un servicio que el Tribunal Contencioso Electoral pone a disposición de sus servidores públicos, para uso estrictamente laboral. Al hacer uso del Internet el usuario debe seguir las siguientes reglas:

- a. Utilizar el Internet apropiadamente, de acuerdo a lo establecido en este Reglamento.
- b. Verificar que la información que acceda en el Internet sea exacta, completa y actual.
- c. El servicio de Internet debe utilizarse exclusivamente para las tareas propias de la función desempeñada en la Institución y no para ningún otro fin.
- d. La utilización del Internet y servicios anexos será únicamente destinado para consulta y verificación de información en sitios considerados de apoyo al desempeño de actividades propias del cargo que desempeña el servidor del Tribunal Contencioso Electoral.
- e. Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la Institución.
- f. La Unidad de Tecnología e Informática tendrá la obligación de limitar a los usuarios el acceso a portales, aplicaciones o servicios de Internet y la Web que pudieren perjudicar los intereses, la productividad y la reputación de la Institución. Específicamente, se bloqueará el acceso por medio de dispositivos fijos y/o móviles a todos aquellos sitios no considerados útiles en el desempeño de las funciones del servidor del Tribunal Contencioso Electoral, en base a los perfiles del puesto; y, el acceso a portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo,



violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses y valores de la Institución o que impacten negativamente en la productividad y trabajo de sus servidores (como mensajería instantánea-chats, redes sociales, video, otros), particularmente a los que atenten a la ética, la moral y buenas costumbres. La Unidad de Comunicación Social es la responsable de administrar las cuentas de redes sociales de la institución, por tal motivo esta dirección tendrá habilitado el acceso a los sitios o portales Web de redes sociales.

- g. Los usuarios no deben utilizar el servicio de Internet mediante los recursos informáticos o de red del Tribunal Contencioso Electoral con fines recreativos o de entretenimiento.
- h. Queda totalmente prohibido el uso de programas como aTube Catcher, Emule, Ares, Kazaa y cualquier otro programa P2P (Peer to Peer).
- i. No se deberá buscar, hacer uso o apoderarse de información personal, ni se deberán obtener copias del software, archivos, datos ni contraseñas pertenecientes a otros usuarios de Internet. No se deberá llevar a cabo en ningún caso la suplantación de forma voluntaria y consciente de otro usuario.
- j. El usuario no debe descargar del internet ningún programa (software) tales como: Shareware, software de valuación, etc., archivos de música (MP3, WAV, MPEG-2, MPEG-4).
- k. El usuario queda prohibido de instalar algún tipo de programa para escuchar MP3, RAR, WAV, o emisoras de radio vía Internet (Winamp, REAL AUDIO, MUSIC MATCH, Oozic PLAYER), sin la autorización de su inmediato superior.
- l. Quedan estrictamente prohibidas las redes de tipo social (Facebook, Hi5, twitter, etc.), sin la autorización de su inmediato superior, autorización que se hará bajo su responsabilidad, siempre y cuando se justifique que este acceso será usado únicamente con fines laborales.
- m. Queda estrictamente prohibido el acceso a sitios de contenido sexual, terrorismo, descarga de piratería, media on-demand (videos, tv, radios, streaming en general, youtube).
- n. El usuario que acceda a un sitio de contenido no apropiado deberá responsabilizarse por cualquier eventual contagio o desperfecto al equipo informático desde el que se accede al sitio Web mediante Internet, ocasionado por la sola visita a este tipo de sitio.
- o. Queda estrictamente prohibido transmitir información confidencial o de contenido político, obsceno, amenazante u hostigante que atente en contra de la seguridad del Estado y esta Institución.
- p. El horario de uso del servicio de Internet es libre y estará disponible las 24 (veinticuatro) horas del día, los 365 días del año en la medida de lo posible, considerando además que se realizarán mantenimientos planificados, o en el caso de suspensión del servicio de Internet por caso fortuito o fuerza mayor. En caso de existir alguna falla en el servicio el usuario deberá reportar el inconveniente a la Unidad de Tecnología e Informática.
- q. La Máxima Autoridad o su delegado autorizará a los servidores del Tribunal Contencioso Electoral el acceso a sitios Web en Internet u otros servicios informáticos, los cuáles no se encuentren permitidos, con la debida justificación del Jefe de la unidad administrativa en la que trabaja el servidor.
- r. El titular de cada unidad podrá requerir acceso a sitios bloqueados de internet indicando los motivos que justifiquen su requerimiento.
- s. El consumo de ancho de banda por usuario será monitoreado y en casos de encontrar un consumo excesivo por varias ocasiones, queda a discreción de la Unidad de Tecnología e Informática solicitar la justificación del mismo al titular de la unidad, de considerarlo conveniente, a fin de analizar y tomar las medidas del caso.
- t. Comprobar (de ser posible) la validez de la información encontrada. En el caso de ser información de otras instituciones, se requerirá que se confirme la información obtenida por internet mediante solicitud escrita o por correo electrónico.
- u. Respetar las protecciones legales de los datos y software proporcionados por sus derechos de autor y licencias.
- v. Informar inmediatamente a la Unidad de Tecnología e Informática sobre cualquier ocurrencia inusual que suceda en el uso de este servicio.

El jefe de cada Despacho de Juez, Dirección o Unidad reportará el uso inadecuado de Internet o el acceso a páginas no autorizadas a la Unidad de Tecnología e Informática, con la finalidad de que se investigue si efectivamente ha existido mal uso del servicio de Internet, y de ser el caso, se restrinja el acceso a dichas



páginas al infractor. El jefe de cada Despacho de Juez, Dirección o Unidad, velará por el cumplimiento de las normas del presente Reglamento por parte del personal a su cargo.

De igual manera, si la Unidad de Tecnología e Informática detectare el mal uso que se le dé al servicio de Internet por parte de un usuario, informará al jefe de cada Despacho de Juez, Dirección o Unidad sobre el hecho, con la finalidad de que se investigue y de ser el caso se restrinja el acceso a páginas no autorizadas.

El mal uso que se le dé al servicio de Internet, por inobservancia de deberes, prohibiciones y obligaciones, por parte de un usuario de esta Institución, dará lugar a la sanción administrativa correspondiente, que se impondrá respetando en todo momento el debido proceso y el derecho a la legítima defensa.

Art. 71.- Aplicación de las políticas de uso de Internet.- La infracción a las obligaciones establecidas en este Reglamento podrán ser sancionadas de conformidad a lo dispuesto en la Ley Orgánica del Servicio Público (LOSEP), respetando en todo momento el debido proceso y el derecho a la legítima defensa.

La Unidad de Tecnología e Informática velará por el cumplimiento de estas políticas, resguardando los intereses de la Institución.

La Unidad de Tecnología e Informática no se hará responsable por incidentes producidos por el incumplimiento del presente Reglamento.

Capítulo VII

SISTEMA DE GESTION DOCUMENTAL QUIPUX

Art. 72.- Definición.- El Sistema de Gestión Documental es una herramienta tecnológica, puesta a disposición de todas las entidades públicas, para efectivizar y agilizar el manejo de información y documentación. El sistema de gestión documental Quipux tiene las siguientes características técnicas:

- a. Conservación intacta de los documentos a lo largo del tiempo;
- b. Acceso inmediato a los documentos independientemente del lugar geográfico;
- c. Búsqueda de documentos definiendo criterios de acceso de forma flexible y fácil;
- d. Consulta simultánea de varios lectores, reproducción;
- e. Envío de documentos obviando el traslado físico;
- f. Inviolabilidad de la información a través de mecanismos de seguridad digital;
- g. Minimización de tiempos de distribución y consulta;
- h. Ahorro de recursos físicos y económicos para gestionar los documentos;
- i. Disminución de impresión de documentos; y,
- j. Apoyo a la conservación del ambiente.

Los manuales para el usuario del Sistema de Gestión Documental Quipux podrán consultarse en la ruta <http://www.gestiondocumental.gob.ec>.

Art. 73.- Administración del sistema.- El Presidente del Tribunal Contencioso Electoral o su delegado, designará al servidor de la Institución que tendrá a su cargo la Administración del Sistema de Gestión Documental Quipux, el cual tendrá acceso al sistema únicamente con los límites establecidos por la Secretaría Nacional de la Administración Pública.

Se garantizará que todos los documentos permanezcan completos, fiables, en cuanto al contenido; auténticos, en cuanto a la originalidad; y accesibles, en cuanto a su localización y legibilidad.

Los documentos digitales tendrán una marca de tiempo que asegure el tiempo exacto de cada operación realizada y la vigencia de la firma electrónica si los mismos hubiesen sido firmados digitalmente.

Art. 74.- Obligaciones de la Unidad de Tecnología e Informática.- Se considerarán como sus obligaciones las siguientes:



- a. Coordinar con la Unidad de Administración de Talento Humano y demás áreas involucradas a fin de identificar y confirmar los servidores del Tribunal Contencioso Electoral a los cuales se les deberá crear un usuario en el Sistema de Gestión Documental Quipux, para el ejercicio de sus funciones.
- b. Definir los perfiles de los servidores del Tribunal Contencioso Electoral que utilicen el Sistema de Gestión Documental Quipux.
- c. Estandarizar las plantillas (institucional/área), que se utilizará para cada documento interno o externo que se genere en el Tribunal Contencioso Electoral.

Art. 75.- Atribuciones del Administrador del Sistema de Gestión Documental.- El servidor del Tribunal Contencioso Electoral, que haya sido nombrado como Administrador del Sistema de Gestión Documental Quipux, tendrá las siguientes obligaciones, mismas que ejecutará a través del área tecnológica:

- a. Crear usuarios en el sistema, áreas de la Institución, así como actualizar los cargos y datos de los servidores del Tribunal Contencioso Electoral, de acuerdo a la información remitida por la Unidad de Administración de Talento Humano.
- b. Asignar los perfiles correspondientes a cada servidor del Tribunal Contencioso Electoral en base a la información remitida por la Unidad de Administración de Talento Humano.
- c. Administrar los accesos para el archivo virtual y físico de documentación e información, según lo definido por la Unidad de Administración de Talento Humano.
- d. Administrar el reinicio de claves de los servidores del Tribunal Contencioso Electoral.
- e. Coordinar con la Unidad de Tecnología e Informática la carga de información actual al sistema de gestión documental Quipux.
- f. Ejecutar los procedimientos relacionados con la subrogación de cargos, cuya información será suministrada por la Unidad de Administración de Talento Humano.
- g. Determinar opciones generales las cuales están asociadas a todos los perfiles, así como también opciones específicas que han sido definidas para cada perfil.

Art. 76.- Accesibilidad y confidencialidad.- Estará delimitada conforme al nivel de acceso que disponga el usuario en el sistema y en los documentos, acceso que depende de la jerarquía, nivel de responsabilidad y permisos. Un documento podrá ser calificado como confidencial para restringir su acceso.

Capítulo VIII

SISTEMAS INFORMÁTICOS JURISDICCIONALES

Art. 77.- Definición.- Los sistemas informáticos jurisdiccionales son herramientas tecnológicas bajo plataforma Web puestas a disposición de los servidores para el ingreso, tratamiento y reporte de información jurisdiccional, mediante perfiles de usuario y roles específicos.

Art. 78.- Administración.- El responsable de la Unidad de Tecnología e Informática tendrá a su cargo la administración, control, respaldo y optimización de los servidores de cómputo donde reposan los sistemas informáticos jurisdiccionales habilitados.

El Secretario General del Tribunal Contencioso Electoral conjuntamente con el responsable de la Unidad de Tecnología e Informática, garantizarán el uso, gestión y disposición de la información contenida en los mismos; en tal razón, avalarán que toda la información permanezca completa y fiable; auténtica, en cuanto a la originalidad; y accesibilidad, en cuanto a su localización e integridad.

Los tiempos de conservación o depuración de la información deberá ser establecida por la Máxima Autoridad o su delegado.

Art. 79.- Modificaciones.- Cualquier modificación a los sistemas informáticos jurisdiccionales deberá ser evaluada por la Unidad de Tecnología e Informática desde el punto de vista de viabilidad técnica y luego ser aprobada por la Máxima Autoridad o su delegado, previo informe del Comité de Seguridad de la Información.



Art. 80.- Desarrollos.- Cualquier desarrollo respecto de sistemas informáticos jurisdiccionales deberá ser evaluado por la Unidad de Tecnología e Informática y aprobado por la Máxima Autoridad o su delegado, bajo los siguientes aspectos:

Área requirente

Entrega de flujos de acciones del sistema con sus respectivos datos de entrada, procesamiento y reportes del mismo; y, entrega del cronograma propuesto donde se contemplen tiempos de desarrollo, implementación, pruebas, optimización y puesta en producción de la herramienta.

Área administrativa-técnica

Disponibilidad de personal, disponibilidad de hardware y viabilidad técnica.

En caso de cumplir los plazos y disponibilidades técnicas planteadas por el área requirente y área administrativa-técnica, se entregará un cronograma de actividades adaptado a los tiempos planteados o consensuados con el área requirente.

Capítulo IX

SISTEMAS INFORMÁTICOS ADMINISTRATIVOS

Art. 81.- Definición.- Los sistemas informáticos administrativos, son herramientas tecnológicas bajo plataforma Web, puestas a disposición de los servidores que conforman la Institución para el ingreso, tratamiento y reporte de información almacenada, mediante perfiles de usuario y roles específicos.

Art. 82.- Administración.- El responsable de la Unidad de Tecnología e Informática tendrá a su cargo la administración, control, respaldo y optimización de los servidores de cómputo donde reposan los sistemas informáticos administrativos.

El Director Administrativo Financiero y el responsable de la Unidad de Tecnología e Informática, en forma conjunta, garantizarán el uso, gestión y disposición de la información contenida en los sistemas informáticos administrativos; en tal razón, avalarán que toda la información permanezca completa y fiable; auténtica, en cuanto a la originalidad; y accesibilidad, en cuanto a su localización e integridad.

Art. 83.- Modificaciones.- Cualquier modificación a los sistemas informáticos administrativos deberá ser evaluada por la Unidad de Tecnología e Informática desde el punto de vista de viabilidad técnica y luego ser aprobada por el Director Administrativo Financiero, previo informe del Comité de Seguridad de la Información.

Art. 84.- Desarrollos.- Cualquier desarrollo respecto de sistemas informáticos administrativos deberá ser evaluado por la Unidad de Tecnología e Informática en conjunto con el Director Administrativo Financiero, una vez que los mismos hayan sido elaborados por las áreas requirentes, bajo los siguientes aspectos:

Área requirente

Entrega de flujos de acciones del sistema con sus respectivos datos de entrada, procesamiento y reportes del mismo; y, entrega de cronograma propuesto donde se contemplen tiempos de desarrollo, implementación, pruebas, optimización y puesta en producción de la herramienta.

Área administrativa-técnica

Disponibilidad de personal, disponibilidad de hardware y viabilidad técnica.

En caso de cumplir los plazos y disponibilidades técnicas planteadas por el área requirente y área administrativa-técnica, se entregará un cronograma de actividades adaptado a los tiempos planteados o consensuados con el área requirente.



Capítulo X
CONTROL

Art. 85.- Claves de acceso.- La Unidad de Tecnología e Informática, conjuntamente con Servicios Generales son responsables de la asignación y la administración de la asignación de claves de acceso a los recursos tecnológicos de la Institución.

Art. 86.- RespalDOS.- La Unidad de Tecnología e Informática estará encargada de generar procesos de respaldo diarios de los buzones para autoridades del Tribunal Contencioso Electoral, siempre y cuando el usuario no los haya descargado a su equipo. Este servicio está configurado con alertas automáticas al alcanzar el umbral del 75% del tamaño de buzón y notificar a los servidores del Tribunal Contencioso Electoral la limpieza de los mismos.

Art. 87.- Responsabilidades.- Los servidores a quienes se autorice la entrega y uso de los bienes, equipos, sistemas informáticos, el correo electrónico institucional, los dispositivos móvil - USB y cualquier otro servicio o sistema, serán responsables de su cuidado, buen uso, destino y conservación, durante el período de tiempo de su gestión o el tiempo que les fuere autorizado su utilización, o la vigencia del respectivo contrato o nombramiento.

Los servidores que hagan uso de los bienes, equipos, sistemas informáticos del correo electrónico institucional, los dispositivos móvil - USB y cualquier otro servicio o sistema, tendrán la obligación de conocer y acatar cualquier instrucción administrativa que se emita sobre el uso y conservación de los mismos, que solo podrán ser utilizados con fines lícitos e inherentes a las actividades oficiales y funciones propias de la Institución, para lo cual informarán oportunamente y por escrito a la Dirección Administrativa Financiera, sobre cualquier novedad que se presente con relación a los mismos o la contravención a las disposiciones contenidas en este instrumento, a fin de adoptar las medidas correctivas que fueren pertinentes para el caso.

De verificarse que algún servidor use los bienes, equipos, sistemas informáticos del correo electrónico institucional, los dispositivos móvil - USB, del servicio de Internet y cualquier otro servicio o sistema provisto por la Institución, para fines ajenos al servicio público o con accesos no autorizados, el custodio o responsable de los mismos deberá justificar dicha situación ante la Dirección Administrativa Financiera, quien a través de la Unidad de Tecnología e Informática levantará un informe donde se determinen los correctivos a tomarse, se establezcan recomendaciones o se determinen responsabilidades o la posible determinación de sanciones administrativas a quienes hubieren incurrido en estos hechos, previo la presentación de los descargos correspondientes y el cumplimiento del debido proceso a cargo de la Unidad de Administración de Talento Humano.

Art. 88.- Responsabilidad de la Unidad de Tecnología e Informática.- Son sus responsabilidades las siguientes:

- a. Mantener los respaldos de la información procesada y almacenada en los equipos y sistemas durante el tiempo que establezca la normativa legal aplicable.
- b. Entregar a cada usuario las herramientas tecnológicas necesarias para su trabajo.
- c. Realizar control de la utilización de recursos tecnológicos e informar a la Unidad de Administración de Talento Humano sobre el mal uso de los mismos por parte del usuario.
- d. Poner a disposición de los servidores del Tribunal Contencioso Electoral un sistema de soporte técnico con el fin de gestionar la solución de problemas y llevar un control de los mismos para garantizar la integridad, confidencialidad y disponibilidad de la información.
- e. Difundir las regulaciones adoptadas en el presente instrumento, a través de circulares u otros medios que considere conveniente para una efectiva socialización al personal del Tribunal Contencioso Electoral previo a su ejecución.
- f. Monitorear permanentemente los accesos a la red institucional de datos y en caso de ser necesario con la colaboración de expertos informáticos externos.
- g. Las demás responsabilidades establecidas en el presente Reglamento a la Unidad de Tecnología e Informática u otras normas aplicables a los procesos de gestión a su cargo.



Capítulo XI
PROHIBICIONES

Art. 89.- Prohibiciones.- Se prohíbe a los servidores del Tribunal Contencioso Electoral lo siguiente:

- a. El uso para actividades particulares de los bienes, equipos, sistemas informáticos, el sistema de correo electrónico institucional y cualquier otro servicio o sistema provisto por la Institución.
- b. El acceso, manejo, intercambio o transmisión de material obsceno u ofensivo, a través de los sistemas informáticos, computacionales o del sistema de comunicación electrónica, el acceso a material erótico, realizar a través de ellos bromas de cualquier forma o cualquier comentario que pueda constituir un acto discriminatorio o de hostigamiento sexual.
- c. El intercambio de archivos con contenidos ajenos a las funciones que desempeñen los servidores del Tribunal Contencioso Electoral.
- d. La navegación virtual por sitios de Internet relacionados con temas tales como sexo, racismo, guerra, violencia, fundamentalismo, diversión, entretenimiento, redes sociales y en general sitios ajenos a las actividades de los servidores del Tribunal Contencioso Electoral.
- e. El uso del correo electrónico con fines de propaganda, manifestaciones u opiniones religiosas, políticas, partidistas o electorales por parte de servidores del Tribunal Contencioso Electoral.
- f. La entrega del listado de contactos de correo electrónico de servidores del Tribunal Contencioso Electoral a terceros sin el permiso de la autoridad competente, previa justificación correspondiente.
- g. La distribución masiva de grandes cantidades de mensajes sean o no de contenido institucional a direcciones externas o dentro de la misma Institución.
- h. El uso de redes sociales, programas de charlas o similares sin la debida autorización de la Unidad de Comunicación Social.
- i. Utilizar o destinar los bienes, equipos, sistemas informáticos, correo institucional, el servicio de Internet inalámbrico y demás bienes o servicios en actos que atenten contra la seguridad del Estado, el orden público, la moral y las buenas costumbres o para realizar actos que desprestigien y afecten a la imagen de la Institución, de sus autoridades y compañeros o para actividades de proselitismo político, comercial o religiosas.
- j. Usar las computadoras, equipos informáticos, internet y sistema de mensajería institucional para propósitos personales, de ocio, para manejo de un negocio o asuntos privados del usuario; para la recepción y envío de mensajes en cadena, para acceder a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro asunto o servicio ajeno a las labores y funciones propias de la Institución.
- k. Copiar, transferir o utilizar en computadoras personales o que no sean de la Institución, programas (software) adquiridos por esta.
- l. Instalar en las computadoras o equipos informáticos programas que no hayan sido adquiridos por la Institución, sin el conocimiento y autorización previa de la Unidad de Tecnología e Informática.
- m. Acceder, utilizar o disponer de información sujeta a propiedad intelectual (copyrighted information) que viole derechos de autor y aquella que sea confidencial o tenga el carácter reservado, sin la debida autorización.
- n. Acceder, utilizar, disponer, alterar o eliminar información de carácter institucional, sin la debida autorización.
- o. Utilizar el Internet inalámbrico a través del módem, USB o similares, para asuntos particulares o que no se relacionen con el trabajo, actividades, funciones o responsabilidades que tienen los funcionarios de la Institución en el ejercicio del cargo asignado.
- p. Egresar o sacar de las oficinas o instalaciones equipos informáticos de propiedad de la Institución, sin la debida autorización de la Dirección Administrativa Financiera.

Capítulo XII
DISPOSICIONES GENERALES

Primera.- La inobservancia de las normas del presente Reglamento será sancionada de conformidad con el régimen disciplinario de Ley Orgánica del Servicio Público, Reglamento General a la Ley Orgánica del



SECRETARÍA GENERAL



Servicio Público, normativa Institucional vigente referente a la materia sin perjuicio de la responsabilidad que pudiere determinarse conforme la Ley Orgánica de la Contraloría General del Estado y otras leyes vigentes.

Segunda.- La Unidad de Tecnología e Informática se encargará de que en cada monitor asignado a servidores o terceros que presten sus servicios para esta Institución, conste de forma obligatoria el logo institucional del Tribunal Contencioso Electoral como protector de pantalla.

En caso de inobservancia a lo dispuesto, o si a sabiendas de lo señalado, servidores del Tribunal Contencioso Electoral o terceros que presten sus servicios para esta Institución, intenten cambiar el protector de pantalla eliminando el logo institucional, la Unidad de Tecnología e Informática notificará al titular de la Dirección Administrativa Financiera a fin de que se proceda con las medidas correctivas pertinentes.

Tercera.- De la sociabilización y ejecución del presente Reglamento, encárguese a la Unidad de Tecnología e Informática.

Cuarta.- Las disposiciones del presente Reglamento son de carácter especial y prevalecerán sobre otras normas de igual o menor jerarquía que se opongan, a excepción de aquellas específicas de la gestión jurisdiccional del Tribunal Contencioso Electoral que no se contemplan expresamente en este instrumento.

Las políticas y procedimientos de archivo para la conservación y mantenimiento de archivos físicos y magnéticos y el instructivo sobre el uso de celulares del Tribunal Contencioso Electoral, expedidos por la Máxima Autoridad, se aplicarán sin oposición a las normas del presente Reglamento.

Quinta.- El presente instrumento entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Sexta.- Encárguese del cumplimiento y de su ejecución a la Dirección Administrativa Financiera y más unidades del Tribunal Contencioso Electoral.

Dado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los veintinueve días del mes de agosto de dos mil diecisiete."

Dado en la ciudad de Quito, Distrito Metropolitano, en la Sala de Sesiones del Pleno del Tribunal Contencioso Electoral, a los veintinueve días del mes de agosto de dos mil diecisiete.- Lo Certifico f).- Ab. Ivonne Coloma Peralta, SECRETARIA GENERAL DEL TRIBUNAL CONTENCIOSO ELECTORAL.

Ab. Ivonne Coloma Peralta
SECRETARIA GENERAL
TRIBUNAL CONTENCIOSO ELECTORAL

Nancy M.

