RESOLUCIÓN PARA APROBAR LA NORMA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN EN EL REGISTRO DE LA PROPIEDAD DEL CANTÓN CUENCA

RESOLUCIÓN No. RA-RPCC-012-2023
Abg. Carlos Eduardo Celi Bravo Mgt.
EL REGISTRADOR DE LA PROPIEDAD DEL CANTÓN CUENCA (E)

CONSIDERANDO

Que, el artículo 66 numeral 19 de la Constitución de la República reconoce y garantiza a las personas: "19. El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de la ley.

Que, la Constitución de la República del Ecuador, en su artículo 83, cuando se refiere a los deberes y responsabilidades de los ecuatorianos, dispone entre otros, el siguiente: "(. . .) 1. Acatar y cumplir la Constitución, la ley y las decisiones legítimas de autoridad competente.

Que, el Ecuador es un Estado Constitucional de Derechos y Justicia según el Art. 1 de la Constitución de la República del Ecuador; por lo tanto, y, en concordancia con el Art. 225 de la Constitución de la República del Ecuador sobre las funciones de las entidades que ejerzan servicios de prestaciones públicas.

Que, el Art. 226 de la Constitución de la República del Ecuador claramente determinada que; “Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultadas que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución”;

Que, la Constitución de la República del Ecuador en el Art. 265 establece: “El sistema público de Registro de la Propiedad será administrado de manera concurrente entre el ejecutivo y las municipalidades”.

Que, el Código de Orgánico Organización Territorial Autonomía y Descentralización COOTAD en su Art 142 establece “…Ejercicio de la competencia de registro de la propiedad. - La administración de los registros de la propiedad de cada cantón corresponde a los gobiernos autónomos descentralizados municipales. P á g i n a 2 | 4 *El sistema público nacional de registro de la propiedad corresponde al gobierno central, y su administración se ejercerá de manera concurrente con los gobiernos*

autónomos descentralizados municipales de acuerdo con lo que disponga la ley que organice este registro. Los parámetros y tarifas de los servicios se fijarán por parte de los respectivos gobiernos municipales..."

El artículo 19 ibídem, de igual forma establece: "*Registro de la Propiedad. - De conformidad con la Constitución de la República, el Registro de la Propiedad será administrado conjuntamente entre las municipalidades y la Función Ejecutiva a través de la Dirección Nacional de Registro de Datos Públicos. Por lo tanto, el Municipio de cada cantón o Distrito Metropolitano se encargará de la estructuración administrativa del registro y su coordinación con el catastro. La Dirección Nacional dictará las normas que regularán su funcionamiento a nivel nacional. Los Registros de la Propiedad asumirán las funciones y facultades del Registro Mercantil, en los cantones en los que estos últimos no existan y hasta tanto la Dirección Nacional de Registro de Datos Públicos disponga su creación y funcionamiento*…"

Que, *el artículo 89 del Código Orgánico Administrativo, establece que* las actuaciones administrativas son: 1. Acto administrativo 2. Acto de simple administración 3. Contrato administrativo 4. Hecho administrativo 5. Acto normativo de carácter administrativo.

Que, *el artículo 130 del Código Orgánico Administrativo determina que: "Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública…".*

Que, el Art. 10 de la Ordenanza para la Organización, Administración y funcionamiento del Registro de la Propiedad del cantón Cuenca establece que "el Registro de la Propiedad del cantón Cuenca como órgano adscrito a la I. Municipalidad, goza de autonomía administrativa, financiera, económica y registral, en conformidad con el Art. 265 de la Constitución de la República del Ecuador y Art. 142 del Código Orgánico de Ordenamiento Territorial, Autonomía y Descentralización. Su función primordial es la inscripción y publicidad de los instrumentos públicos, títulos y demás documentos que la ley exige o permite que se inscriban en los registros correspondientes";

Que, mediante ORDENANZA PARA LA ORGANIZACIÓN, ADMINISTRACIÓN Y FUNCIONAMIENTO DEL REGISTRO DE LA PROPIEDAD DEL CANTÓN CUENCA, en su Título I DE LA O EL REGISTRADOR DE LA PROPIEDAD, en su Artículo 14 establece que "La o el Registrador de la Propiedad del cantón Cuenca, como máxima autoridad administrativa y representante legal y judicial del Registro de la Propiedad del cantón Cuenca…";

Que, la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial No.459, 26 de mayo 2021, en su Art. 1, establece como objeto y finalidad de esta ley, el de garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como

su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

Que, el Art, 2 de la Ley Ibídem señala que la presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior.

Que, el Art. 37 de la Ley Ibídem señala que: "el responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales. El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados. Entre otras medidas, se podrán incluir las siguientes; 1) Medidas de anonimización, seudonomización o cifrado de datos personales; 2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y 3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica. 4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales".

Que, el Art. 38 de la Ley Ibídem determina el mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza., vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los daros conforme al principio de seguridad de datos personales. El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información.

Que, el Art. 45 de la Ley ibídem señala que, para la correcta prestación de los servicios de telecomunicaciones y la apropiada operación de redes de telecomunicaciones, los prestadores de servicios de telecomunicaciones deben garantizar el secreto de las comunicaciones y seguridad de datos personales. Únicamente por orden judicial, los prestadores de servicios de telecomunicaciones podrán utilizar equipos, infraestructuras e instalaciones que permitan grabar los contenidos de las comunicaciones específicas dispuestas por los jueces competentes. Si se evidencia un tratamiento de grabación o interceptación de las comunicaciones no autorizadas por orden judicial se aplicará lo dispuesto en la presente Ley.

Que, la disposición transitoria primera de la ley ibídem determina que, las disposiciones relacionadas con las medidas correctivas y el régimen sancionatorio entrarán en vigencia en dos años contados a partir de la publicación de esta ley en el Registro Oficial, en el transcurso de este tiempo los responsables y encargados del tratamiento, de datos personales se adecuarán a los preceptos establecidos dentro de esas disposiciones, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales.

Que, en el numeral 6 del Art. 20 de la Ley Orgánica de Empresas Públicas, determina: "(---) 6. Confidencialidad en la información comercial, empresarial y en general, aquella información, considerada por el Directorio de la empresa pública como estratégica y sensible a los intereses de ésta, desde el punto de vista tecnológico, comercial y de mercado, la misma que goza de la protección del régimen de propiedad intelectual e industrial, de acuerdo a los instrumentos internacionales y la Ley de Propiedad Intelectual, con el fin de precautelar la posición de las empresas en el mercado; (…).

Que, El Ministro de Telecomunicaciones y de La Sociedad de la Información promulgo el Acuerdo No. 025-2019 que determina el Esquema Gubernamental de Seguridad de La Información –EGSI, mismo que está publicado en la Edición Especial No.228 del 10 de enero 2020 y la última reforma en el Registro Oficial 550, 04- octubre de 2021, misma que es implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Que, el Abg. Carlos Eduardo Celi Bravo Mgt. Registrador de la Propiedad del cantón Cuenca Encargado, autoriza a realizar la resolución a la Dirección de Asesoría Jurídica, para proceder con el encargo y responsabilidad de la Seguridad de la Información del año 2023 del Registro de la Propiedad del cantón Cuenca. Que, la autonomía registral, administrativa y financiera de la que goza el Registro de la Propiedad del cantón Cuenca, como lo establece el Art. 10 de la Ordenanza para la Organización, Administración y Funcionamiento del Registro de la Propiedad del cantón Cuenca, nos permite y en uso de estas atribuciones que le confiere la Ley realizar la presente resolución;

El Registro de la Propiedad del cantón Cuenca por medio de su Máxima Autoridad y en uso de facultades Constitucionales y Legales:

RESUELVE:

Art. 1.- Dar por conocido y aprobar la Norma Técnica de seguridad de la Información del Registro de la Propiedad del Cantón Cuenca:

1 POLÍTICA DE SEGURIDAD

“El Registro de la Propiedad del Cantón Cuenca, garantiza la confidencialidad, integridad y disponibilidad de la Información entregada por las partes interesadas, mediante la aplicación de normas, procedimientos, instructivos y procesos alineados al marco legal vigente, las buenas prácticas de seguridad de la información y la mejora continua del SGSI.”

2 OBJETIVOS

a) Incrementar el nivel de protección de los activos del Registro de la Propiedad del cantón Cuenca (información, recursos, bienes, etc.) para lograr los niveles adecuados de integridad, confidencialidad y disponibilidad de acuerdo a lo dispuesto en el EGSI.

b) Incrementar la adopción y aplicación progresiva de las políticas, estrategias, normas, procedimientos, tecnologías y medios necesarios para asegurar la continuidad operacional de los procesos y servicios que desarrolla el Registro de la Propiedad del cantón Cuenca frente a las amenazas, ya sean internas o externas, deliberadas o accidentales.

c) Reducir al máximo las probabilidades de sufrir violaciones a la seguridad de la información e infraestructura crítica.

3 ROLES Y RESPONSABILIDADES

El Presidente del Comité de Seguridad de la Información (CSI - equipo directivo) es el responsable de asegurar que la seguridad de la información se gestione adecuadamente en el Registro de la Propiedad del cantón Cuenca.

Los Directores, Jefes y otras áreas de liderazgo, son responsables de garantizar que los funcionarios que trabajan bajo su control protejan la información de acuerdo con las normas establecidas por la institución.

El Oficial de Seguridad de la Información asesora al equipo directivo, proporciona apoyo especializado al personal de la institución y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.

Cada uno de los funcionarios de la institución tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo

4 ALCANCE

La Política de Seguridad de la Información y la Norma Técnica se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Registro de la Propiedad del catón Cuenca.

La Seguridad de la Información es un concepto integral, por lo cual, la aplicación de la política de la seguridad, así como la normativa técnica que la acompaña, será transversal a todos los procesos; aplicándose a todo el conjunto de dependencias y recursos (Direcciones, Jefes Departamentales, personal, terceros, externos, contratistas, etc.); debiendo ser conocida y cumplida por todos los empleados, sea cual fuere su nivel jerárquico y su tipo de dependencia laboral, así como también por terceros que requieran acceso o uso a los activos de información del Registro de la Propiedad del cantón Cuenca.

5 COMUNICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información será comunicada mediante talleres, inducciones, publicidad interna usando el correo electrónico, entre otros; a los funcionarios del Registro de la Propiedad del cantón Cuenca, así como a las partes interesadas. La Dirección de Talento Humano se encargará de realizar esta comunicación de manera permanente con acompañamiento del Oficial de Seguridad de la Información.

6 DOCUMENTOS DE REFERENCIA

- Constitución de la República del Ecuador
- Ley Orgánica de Protección de Datos Personales
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000
- Reglamento Interno
- Plan Estratégico

7 TÉRMINOS Y DEFINICIONES

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento se realizan las siguientes definiciones:

Activo: Todo bien que tiene valor para la institución.

Información: Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, conocimientos, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Seguridad de la Información: La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación y la operación normal de la empresa.

Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del organismo, observancia legal e imagen.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Oficial de Seguridad de la Información: será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de esta norma.

Auditoría: revisión e inspección independiente de las medidas de seguridad implantadas para valorar su idoneidad y eficacia, verificando y asegurando su conformidad con las políticas y los procedimientos establecidos y recomendando los cambios necesarios.

Documento: cualquier soporte portátil con capacidad para contener información.

Manejar información: elaborar, presentar, almacenar, procesar, transportar o destruir información.

Necesidad de conocer: determinación positiva por la que se confirma que un posible destinatario requiere el acceso a una determinada información para desempeñar servicios, tareas o cometidos oficiales.

Vulnerabilidad: debilidad, atributo o pérdida de control que permitiría o facilitaría la materialización de una amenaza.

Amenaza: evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales.

Riesgo: la probabilidad o potencialidad de que una vulnerabilidad sea aprovechada por una amenaza, comprometiendo la confidencialidad, integridad y/o disponibilidad.

Sistema de Información y Telecomunicaciones: conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita manejar información.

Autoridad de Protección de Datos Personales: Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.

Delegado de protección de datos: Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable de tratamiento de datos.

Encargado del tratamiento de datos personales: Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

Responsable de tratamiento de datos personales: persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

Titular: Persona natural cuyos datos son objeto de tratamiento.

Destinatario: Persona natural o jurídica que ha sido comunicada con datos personales.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

Vulneración de seguridad de datos personales: Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

Dato biométrico: Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

Dato genético: Dato personal único relacionado a características genéticas heredadas o adquiridas de aún persona natural que proporcionan información única sobre la fisiología o salud de un individuo.

Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.

Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido puedan dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

TLP. Para la determinación de la categorización de la información contenida en los documentos del Registro de la Propiedad del cantón Cuenca se deberá tener en cuenta lo dispuesto en la Constitución de la República del Ecuador, en el artículo 66, numeral 19, relacionada con el derecho a la protección de datos de carácter personal; lo establecido en la Ley Orgánica de Telecomunicaciones Título VIII referente al Secreto de las Telecomunicaciones y Protección de Datos Personales; a lo dispuesto en el Reglamento General a la Ley Orgánica de Telecomunicaciones Titulo XV Secreto a la Comunicación y Protección de Datos; La Ley Orgánica de Protección de Datos Personales, y; las demás leyes y reglamentos que tengan incidencia directa en su operación y funcionamiento.

Se utiliza el protocolo TLP (Traffic Light Protocol o Protocolo de Semáforos) para la categorización del nivel de confidencialidad de los documentos, según el cual quien remite la información, debe categorizarla de acuerdo a uno de los siguientes criterios: Pública General, Pública Comunitaria, Sensible y Confidencial, con base al detalle que se describe a continuación.

Información Pública General (TLP: Blanco – Difusión sin restricción)

La información categorizada con TLP Blanco, es aquella información que el Registro de la Propiedad del cantón Cuenca o sus funcionarios podrá difundir al interior o el público en general. Este tipo de información debe cumplir como mínimo con las siguientes consideraciones:

Su divulgación no representa riesgo para el cliente al cual se relaciona la información

Para su tratamiento no es necesario establecer restricciones especiales, más allá de las recomendaciones sobre el buen uso y conservación de la información.

Su difusión o utilización no transgrede derechos de autor.

Información Pública Comunitaria (TLP Verde – Difusión dentro de la comunidad)

Registro de la Propiedad del cantón Cuenca o sus funcionarios podrán compartir la información con miembros específicos del mismo Registro de la Propiedad del cantón Cuenca o externos de la Comunidad (ejemplo Arcotel u otro proveedor de servicios de internet, etc.) anonimizando la información, para no causar perjuicio al propietario de la misma. Este tipo de información nunca debe ser publicada en internet o cualquier medio al cual el público general pueda acceder de manera directa y sin una solicitud expresa.

Se debe observar la no transgresión de derechos de autor.

Información Sensible (TLP Ámbar – Difusión Limitada)

Este tipo de información debe ser difundida por el Registro de la Propiedad del cantón Cuenca o sus servidores para uso interno y exclusivo de las respectivas Direcciones, Jefaturas y/o con los proveedores o, usuarios que necesitan conocerla, para gestionar dicha información.

El dueño de la información deberá autorizar el uso de la misma cuando se requiera su utilización para un propósito distinto al original. La información que no se encuentre categorizada por defecto será TLP Ámbar.

Se debe asegurar la existencia de controles que garanticen la integridad y seguridad de información Sensible al ser transmitida por cualquier medio.

Se evitará imprimir documentación sensible, más allá de lo estrictamente necesario, por lo cual se recomienda el intercambio de este tipo de información vía correo electrónico.

Información Confidencial (TLP Rojo - Solo para destinatarios específicos)

La información catalogada como confidencial sólo podrá ser difundida por el RPCC o sus funcionarios, a destinatarios específicos de la misma, prohibiéndose la compartición de este tipo de información, incluso a un nivel superior, ya que su difusión fuera del grupo deseado, podría tener un impacto en la privacidad, reputación o en la operación del negocio; si es mal utilizada.

Si la información necesita ser extendida fuera del grupo deseado, se requiere autorización explícita por escrito del dueño de la información.

En general se debe evitar imprimir este tipo de documentos.

La transmisión de este tipo de información deberá ser únicamente a través de medios seguros que garanticen la prohibición de acceso por parte de personas no autorizadas.

8 SANCIONES POR INCUMPLIMIENTO

El incumplimiento de las disposiciones establecidas por la Norma Técnica de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido. Para la aplicación de sanciones al personal se deberá seguir el procedimiento administrativo sancionador que establezca el Reglamento Interno del Registro de la Propiedad del cantón Cuenca para los Servidores de Carrera, Contratados y de Libre Nombramiento y Remoción, no sujetos a la Contratación Colectiva del Registro de la Propiedad del Cantón Cuenca.

9 ESTRUCTURA DE ESTA NORMA

Esta norma está basada en el estándar internacional ISO/IEC 27002, por lo cual contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo.

9.1 Cláusulas

Cada cláusula contiene un número de categorías principales de seguridad. Las 11 cláusulas (acompañadas por el número de categorías principales de seguridad incluidas en cada cláusula) son:

1. Políticas de seguridad de la información (1);
2. Organización de la seguridad de la información (2);
3. Seguridad relativa a los recursos humanos (3);
4. Gestión de activos (3);
5. Control de acceso (4);
6. Criptografía (1);
7. Seguridad física y del entorno (2);
8. Seguridad de las operaciones (7);
9. Seguridad de las comunicaciones (2);
10. Adquisición, desarrollo y mantenimiento de los sistemas de información (3);
11. Relación con proveedores (2);
12. Gestión de incidentes de seguridad de la información (1);

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio (2);
14. Cumplimiento (2)

El orden de las cláusulas en esta norma técnica no tiene relación a su importancia.

9.2 Categorías principales de seguridad

Cada categoría principal de seguridad contiene:

- Un objetivo de control declarando lo que se debe alcanzar.
- Uno o más controles que pueden ser aplicados para alcanzar el objetivo de control.

Cada control a ser aplicado, a su vez se estructura de la siguiente manera:

Control

Define específicamente la declaración de control para satisfacer el objetivo de control.

La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio para la identificación y clasificación de riesgos y que aseguren la reducción de los riesgos a un nivel aceptable.

10. EVALUACIÓN Y TRATAMIENTO DEL RIESGO (CLAUSULA INTRODUCTORIA)

La evaluación de riesgos deberá identificar, cuantificar y priorizar los riesgos contra el criterio para la aceptación de los niveles máximos tolerables y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para la implementación de los controles seleccionados.

La evaluación del riesgo debe incluir un alcance sistemático que permita determinar la probabilidad de ocurrencia e impacto que causaría de llegar a materializarse (análisis del riesgo).

Las evaluaciones del riesgo deben ser realizadas periódicamente para incluir los cambios en los requerimientos del sistema y en la situación del riesgo, por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando cambios significativos ocurran. Estas evaluaciones del riesgo deben ser emprendidas de una forma metódica, capaz de producir resultados comparables y reproducibles.

Antes de considerar el tratamiento de un riesgo, la organización debe decidir el criterio para determinar si es que los riesgos son aceptados o no. Los riesgos pueden ser aceptados si, por ejemplo, se evalúa que el riesgo es menor o que el costo de aplicar los controles no es rentable para la organización. Estas decisiones deben quedar registradas.

Para cada uno de los riesgos identificados, siguiendo la evaluación del riesgo, se necesita realizar una decisión del tratamiento del riesgo. Posibles opciones para el tratamiento del riesgo incluyen:

- Aplicar controles apropiados para reducir riesgos.
- Riesgos aceptados objetivamente y con conocimiento, satisfaciendo claramente el criterio para la aceptación del riesgo y la política de la organización.
- Evitar riesgos no permitiendo realizar acciones que puedan causar que estos ocurran.
- Transferir los riesgos asociados a terceros como son los proveedores y aseguradores.

Los controles en la seguridad de información deben ser considerados en los sistemas y en las especificaciones de las exigencias de los proyectos, así como en la etapa de diseño. Las fallas pueden resultar en costos adicionales y en soluciones menos efectivas y posiblemente, en el peor de los casos, inhabilidad para alcanzar una seguridad adecuada.

11. CONTROLES SEGURIDAD DE LA INFORMACIÓN

Para los controles del Sistema de Gestión de Seguridad de la información se usarán los controles del Anexo A de la norma ISO 27001.

El Oficial de Seguridad de la Información remitirá a cada una de las áreas los controles de los que son responsables y realizará las sugerencias para las Guías de Implementación.

Cada una de las áreas realizará la guía de implementación para los controles que son responsables.

Para la Guía de Implementación las áreas usarán los lineamientos indicados en la Ley Orgánica de Protección de Datos Personales, Esquema Gubernamental de Seguridad de la Información, Normas de Control Interno de Contraloría y otras leyes o normativas propias del tratamiento de la información que sean vinculantes para el Registro de la Propiedad del cantón Cuenca.

A.5 Políticas de seguridad de la información
A.5.1 Directrices de gestión de la seguridad de la información
Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.

A.5.1.1	Políticas para la seguridad de la información	*Control* Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades en seguridad de la información	*Control* Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de tareas	*Control* Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Deben mantenerse los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.
A.6.2 Los dispositivos móviles y el teletrabajo		
Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.		

A.6.2.1	Política de dispositivos móviles	*Control* Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.
A.7 Seguridad relativa a los recursos humanos		
A.7.1 Antes del empleo		
Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.		
A.7.1.1	Investigación de antecedentes	*Control* La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.		
A.7.2.1	Responsabilidades de gestión	*Control* La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	*Control* Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A.7.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.
A.7.3 Finalización del empleo o cambio en el puesto de trabajo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.		
A.7.3.1	Responsabilidades ante la finalización o cambio	*Control* Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.
A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.8.1.1	Inventario de activos	*Control* La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
A.8.1.2	Propiedad de los activos	*Control* Todos los activos que figuran en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

A.8.1.4	Devolución de activos	*Control* Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
A.8.2.2	Etiquetado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.2.3	Manipulado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3 Manipulación de los soportes		
Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.		
A.8.3.1	Gestión de soportes extraíbles	*Control* Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de soportes	*Control* Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
A.8.3.3	Soportes físicos en tránsito	*Control* Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Limitar el acceso a los recursos de tratamiento de la información y a la información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de red	*Control* Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A.9.2 Gestión de acceso de usuario		
Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuario	*Control* Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
A.9.2.2	Provisión de acceso de usuario	*Control* Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.9.2.3	Gestión de privilegios de acceso	*Control* La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	*Control* La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A.9.2.5	Revisión de los derechos de acceso de usuario	*Control* Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.

A.9.2.6	Retirada o reasignación de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.		
A.9.3.1	Uso de la información secreta de autenticación	*Control* Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	*Control* Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A.9.4.4	Uso de utilidades con privilegios del sistema	*Control* Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.
A.10 Criptografía		
A.10.1 Controles criptográficos		

Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		
A.10.1.1	Política de uso de los controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
A.10.1.2	Gestión de claves	*Control* Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A.11 Seguridad física y del entorno		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
A.11.1.2	Controles físicos de entrada	*Control* Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A.11.1.3	Seguridad de oficinas, despachos y recursos	*Control* Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
A.11.1.4	Protección contra las amenazas externas y ambientales	*Control* Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
A.11.1.5	El trabajo en áreas seguras	*Control* Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.

A.11.1.6	Áreas de carga y descarga	*Control* Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.
A.11.2 Seguridad de los equipos		
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de equipos	*Control* Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.
A.11.2.2	Instalaciones de suministro	*Control* Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
A.11.2.3	Seguridad del cableado	*Control* El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A.11.2.4	Mantenimiento de los equipos	*Control* Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A.11.2.5	Retirada de materiales propiedad de la empresa	*Control* Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	*Control* Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.
A.11.2.7	Reutilización o eliminación segura de equipos	*Control* Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera

		segura, antes de deshacerse de ellos.
A.11.2.8	Equipo de usuario desatendido	*Control* Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	*Control* Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.		
A.12.1.1	Documentación de procedimientos operacionales	*Control* Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	*Control* Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de capacidades	*Control* Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	*Control* Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
A.12.2 Protección contra el software malicioso (*malware*)		
Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el *malware*.		

A.12.2.1	Controles contra el código malicioso	*Control* Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A.12.3 Copias de seguridad		
Objetivo: Evitar la pérdida de datos		
A.12.3.1	Copias de seguridad de la información	*Control* Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A.12.4 Registros y supervisión		
Objetivo: Registrar eventos y generar evidencias.		
A.12.4.1	Registro de eventos	*Control* Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
A.12.4.2	Protección de la información del registro	*Control* Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
A.12.4.3	Registros de administración y operación	*Control* Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.
A.12.4.4	Sincronización del reloj	*Control* Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.
A.12.5 Control del software en explotación		
Objetivo: Asegurar la integridad del software en explotación.		
A.12.5.1	Instalación del software en explotación	*Control* Se deben implementar procedimientos para controlar la instalación del software en explotación.

A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
A.12.6.2	Restricción en la instalación de software	*Control* Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre la auditoria de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		
A.12.7.1	Controles de auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.		
A.13.1.1	Controles de red	*Control* Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A.13.1.3	Segregación en redes	*Control* Los grupos de servicios de información, los usuarios y los sistemas de información deben estar

		segregados en redes distintas.
A.13.2 Intercambio de información		
Objetivo: Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de intercambio de información	*Control* Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
A.13.2.2	Acuerdos de intercambio de información	*Control* Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.
A.13.2.3	Mensajería electrónica	*Control* La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
A.13.2.4	Acuerdos de confidencialidad o no revelación	*Control* Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.14.1 Requisitos de seguridad en los sistemas de información		
Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.		
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	*Control* Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	*Control* La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizados.

A.14.1.3	Protección de las transacciones de servicios de aplicaciones	*Control* La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizada.
A.14.2 Seguridad en el desarrollo y en los procesos de soporte		
Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.
A.14.2.2	Procedimiento de control de cambios en sistemas	*Control* La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	*Control* Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.
A.14.2.4	Restricciones a los cambios en los paquetes de software	*Control* Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.
A.14.2.5	Principios de ingeniería de sistemas seguros	*Control* Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.
A.14.2.6	Entorno de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.

A.14.2.7	Externalización del desarrollo de software	*Control* El desarrollo de software externalizado debe ser supervisado y controlado por la organización.
A.14.2.8	Pruebas funcionales de seguridad de sistemas	*Control* Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	*Control* Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos de prueba		
A.14.3.1	Protección de los datos de prueba	*Control* Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.
A.15 Relación con proveedores		
A.15.1 Seguridad en las relaciones con proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	*Control* Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.
A.15.1.2	Requisitos de seguridad en contratos con terceros	*Control* Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información.
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	*Control* Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

A.15.2 Gestión de la provisión de servicios del proveedor		
Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores		
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	*Control* Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	*Control* Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
A.16.1.2	Notificación de los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.
A.16.1.3	Notificación de puntos débiles de la seguridad	*Control* Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	*Control* Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.

A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	*Control* El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.
A.16.1.7	Recopilación de evidencias	*Control* La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.
A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementar la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias.		
Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.		

A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	*Control* Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.
A.18.1.2	Derechos de Propiedad Intelectual (DPI)	*Control* Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
A.18.1.3	Protección de los registros de la organización	*Control* Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.
A.18.1.4	Protección y privacidad de la información de carácter personal	*Control* Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.
A.18.1.5	Regulación de los controles criptográficos	*Control* Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.
A.18.2 Revisiones de la seguridad de la información		
Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.		

A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	*Control* Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable
A.18.2.3	Comprobación del cumplimiento técnico	*Control* Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

DISPOSICIÓN DEROGATORIA. - Deróguese toda normativa interna de igual o menor jerarquía que se oponga a las disposiciones contenidas en esta norma técnica.

DISPOSICIONES TRANSITORIAS:

Primera. - El presente instructivo deberá ser difundido a todos los servidores públicos de la Institución, a través del Oficial de Seguridad de la Información, en un plazo no superior a los 60 días a partir de su fecha de promulgación.

Disposición Final: La presente Resolución entrará en vigencia a partir de la fecha de su suscripción.

Art 2.- Disponer a la **Jefatura de Tecnologías de la Información de Comunicación,** se proceda a la publicación de la **RESOLUCIÓN PARA DETERMINAR LA NORMA TECNICA DE SEGURIDAD DE LA INFORMACIÓN EN EL REGISTRO DE LA PROPIEDAD DEL CANTÓN CUENCA del año 2023**, con sus anexos en la página WEB del Registro de la Propiedad del cantón Cuenca, conforme lo establece el inciso segundo del Art. 22 de la LOSNCP.

Dado y firmado en el Registro de la Propiedad del cantón Cuenca, el 23 de mayo del 2023.

Firmado electrónicamente por:
CARLOS EDUARDO CELI BRAVO

Abg. Carlos Eduardo Celi Bravo Mgt.
REGISTRADOR DE LA PROPIEDAD DEL CANTÓN CUENCA ENCARGADO

Control Legal:	Abg. Stalin Wladimir Bravo Muñoz Mgt. **DIRECTOR DE ASESORÍA JURIDÍCA.**	Firmado electrónicamente por: STALIN WLADIMIR BRAVO MUNOZ